PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-225143

(43)Date of publication of application : 17.08.1999

(51)Int.Cl. H04L 9/32
G06F 17/60
G06K 17/00
G07B 1/00
G07B 5/00
G07F 7/12
G09C 1/00

(21)Application number : 10-027074

(22)Date of filing : 09.02.1998

(71)Applicant : FUJI XEROX CO LTD

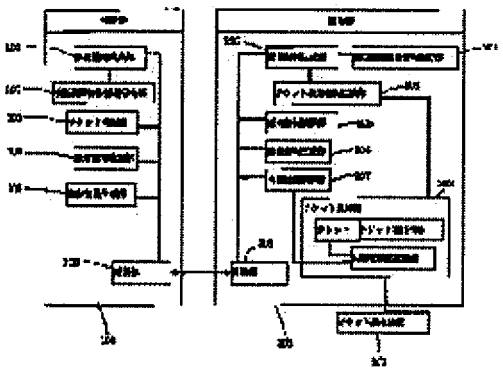
(72)Inventor : KIKO KENICHIROU
NAKAGAKI JUHEI
KIYOUJIMA HITOKI
TANIGUCHI SHINICHIRO

(54) ELECTRONIC TICKET SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an internal state of a certificate device from being revised due to a ticket exhibited by mistake or illegally.

SOLUTION: An authentication information generating section 102 of an authentication device 100 generates authentication information and sends it to a certificate device 200. A ticket discrimination information generating section 203 of the certificate device 200 generates ticket discrimination information to indicate storage of a correct ticket from ticket utilization information and information in an internal state storage area. A certificate information generating section 206 connects ticket discrimination information to low-order bits of a bit stream of the authentication information to generate ticket certificate information. The ticket certificate information is sent to the authentication device 100 by a communication section 208. The authentication device 100 receiving the ticket certificate information conducts ticket discrimination processing and



terminates the protocol when the ticket certificate information is incorrect or the ticket is not to be authenticated.

LEGAL STATUS

[Date of request for examination]	20.09.2002
[Date of sending the examiner's decision of rejection]	23.08.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the technique of creating a ticket and a card electronically and using them.
[0002]
[Background of the Invention] The attempt which publishes common tickets, such as a ticket, an admission ticket, a reserved seat ticket, a reservation ticket, a coupon ticket, a commuter pass, a prepaid card, and a point card, as an electronic ticket is performed in recent years [[conventional technical]].
[0003] A publisher can specify the right granted to the user and such an electronic ticket has the function in which it is verifiable that it is a right ticket. Electronic intelligence is easy to create, and although it has the features that it can transmit through a communication line, since a perfect copy can be made easily, the cure to the unjust use by forgery and the duplicate is indispensable to implementation of an electronic ticket. Although prevention of forgery by electronic signature is possible, prevention of a duplicate is difficult, and preventing the unjust use by the duplicate had become the biggest technical problem were in charge of implementation of an electronic ticket.
[0004] The three approaches of of the user just to the utilization time of the former and a ticket as a solution, the 1st conventional technique to check, the 2nd conventional technique which does not give an opportunity to copy a ticket at persons other than a publisher, and the 3rd conventional technique which corrected the 2nd conventional technique so that the communication link at the time of verification could be exhibited over this problem have been proposed.
[0005] The 1st conventional technique is the approach a user checks whether you are a just user to the utilization time of a ticket, and a user shows with a ticket that he is the just user to whom he suits user specific information, when using a ticket. If it conforms to user specific information, use of a corresponding right will be accepted. Information which matches information (user specific information) required for a check and the granted right is published as a ticket, and a user keeps records. In order for persons other than a publisher to prevent from forging a ticket freely, a publisher performs electronic signature to a ticket. The ticket without electronic signature is judged to be what was forged. Possession of the knowledge of the bodily features of an identity, a photograph of his face, etc., a password, etc. can be used for user specific information.
[0006] However, by this approach, some troubles arise according to the user specific information to be used.
[0007] For example, by the approach of using a user's identity for user specific information, a user will be identified at the time of issue and verification, and anonymity will be lost. Moreover, since the method of proving a status safely in the remote environment using a communication line is not realized, in such an environment, a thing without a just right cannot prevent using a ticket unfairly.
[0008] Although the problem of anonymity will be mitigated if a password is used for user specific information, the load which memorizes a password is given to a user. Moreover, since it cannot prevent that a user makes a password reveal intentionally, there is also a trouble that the risk of unjust use will

increase.
[0009] The 2nd conventional technique is the approach of not giving an opportunity copying a ticket to persons other than a publisher as is shown in JP,8-147500,A. By this approach, both the device which prevents from copying the ticket in which the user is doing maintenance management, and the device which a ticket does not reveal from the communication link at the time of issue and verification are needed.
[0010] However, by this approach, since persons other than (1) publisher also carry out the contents of the communication link at the time of issue of (2) tickets with which it becomes difficult to prove the justification of a ticket for a third person since a ticket cannot be copied, and verification to secrecy, the trouble that it cannot prove not infringing on the right of users, such as privacy, at the time of issue of a ticket and verification arises.
[0011] The 3rd conventional technique is the approach which corrected the 2nd conventional technique so that the communication link at the time of verification can be exhibited, as shown in JP,6-52518,B. Although it records that it cannot copy to the equipment (certification equipment) which a user possesses by making a ticket into confidential information like the 2nd conventional technique by this approach, the approaches of verification differ. First, the verification equipment which verifies sends values (challenge) by which repeat use is not carried out, such as a random number, to certification equipment. Certification equipment performs the operation using the confidential information which is a ticket to a challenge, and returns the acquired value (response) to verification equipment. Verification equipment is checking what the response's calculated using confidential information and a challenge, and attests a user's justification. It becomes unnecessary to let a challenge and a response be secret communication by making it difficult in computational complexity to ask for confidential information conversely from a response.
[0012] This approach is used for authentication and information is not transmitted [whether the just ticket is held and] to except. For this reason, an expiration date etc. cannot be shown but only a simple ticket can be expressed. Moreover, there was a problem that it could not prove that the method of transmitting a ticket to certification equipment needs to carry out by secret communication link like the 2nd conventional technique, discloses a user's information unfairly, and is not infringing on a user's right.
[0013] Thus, each Prior art had a problem in the point at the sacrifice of the function of a ticket of contents certification and a user's anonymity to a third person, in order to realize the function to prevent unjust use required for a ticket.
[0014] [Related technique] The approach shown in Japanese Patent Application No. No. (un-opening [July 14, Heisei 9,] to the public) 188064 [nine to] is proposed as a related technique which solves these problems.
[0015] The general Challenge Handshake Authentication Protocol of this related technique is shown in drawing 1 . This protocol is a protocol which performs bidirectional authentication, and when both sides check the signature to authentication information (generated random number), it attests each other justification. Informational safe transfer is enabled by including a message (m, mu) in a part of mutual authentication information (random number).
[0016] The protocol of a related technique is explained with reference to drawing 1 . In drawing 1 , first, verification equipment generates the authentication information C based on a random number (S11), and this authentication information C is sent to certification equipment (S12). On the other hand, certification equipment generates another authentication information chi based on a random number, and sends the authentication information chi to verification equipment (S13, S14). Corresponding to a ticket, there is an internal state which cannot be operated in certification equipment from the exterior, and it can rewrite only by the response indication from verification equipment. The response indication in which the information (mu) to which modification of an internal state is permitted was included is created to a part of chi, verification equipment signs it, and verification equipment is sent to it at certification equipment (S15, S16). By checking the signature of a response indication rho, a transmitting person checks that it is just verification equipment, and, as for certification equipment, checks the rightness of

the information mu on internal-state modification with it (S17). The internal state of certification equipment is changed only into a right case for rho according to the contents of mu (S18). The service set to verification equipment by performing a signature it being possible to restore D (S19) and according to D to the certification information R at the last when delivery (S20, S21) and verification equipment checked the signature is offered from Ticket t and the certification equipment proper information du that certification equipment was created justly (S22, S23).

[0017] According to this approach, since the verification information on a ticket is public presentation, verification of a ticket is possible for it also to the 3rd person, and since a user does not have the need of showing the information which specifies a user at the time of verification of a ticket, anonymity is also kept.

[0018] Moreover, when verification equipment and certification equipment share each of each other's confidential information and public information and carry out mutual authentication, the problem of forgery of certification equipment and verification equipment is solved. Furthermore, by embedding information transmitting to a part of authentication information used for this certification, signal transduction verification equipment and between certification equipment is also made possible, and the contents of the ticket can be proved.

[0019] Thus, if the approach of this related technique is used, the safe electronic ticket which filled all the fundamental functions of an electronic ticket can be realized, and it is possible to solve all the above-mentioned problems.

[0020] By the way, with the previous related technique, it is premised on the ticket which verification equipment tends to verify becoming settled uniquely in certification equipment by sending the information as which verification equipment specifies a ticket to certification equipment. However, it is also considered in fact that two or more tickets verifiable [with the verification equipment] exist in certification equipment. For example, when a thing like the ticket of a railroad is considered, two or more tickets, such as a valid coupon ticket, a valid commuter pass, etc., may exist in certification equipment from the station. In such a case, with certification equipment, it cannot judge which ticket the user is going to use. Then, the need of choosing the ticket which a user uses beforehand in such cases arises.

[0021] And in such a scene, if a previous related technique is applied, the problem that it will be created and the response indication to which modification of the internal state corresponding to a ticket is permitted will be sent, without checking the contents of the ticket chosen and shown will arise.

[0022] This means that the internal state of the ticket which is not meant will be changed, when the ticket which the user mistook has been chosen.

[0023] Moreover, considering the case where it applies to the ticket of a railroad, it is possible by leaving record of entrance and checking record of entrance as an internal state, at the time of participation to prevent a malfeasance like cheating on the fare.

[0024] Here, a case so that it may leave only the fact of having only come in to the internal state corresponding to a ticket, as information on entrance is considered. In such a case, if it sends to certification equipment, without checking the modification authorization information on an internal state, and the contents of the ticket specifically shown entrance information, originally it will become possible to leave the fact of having come in at the station also to the ticket which cannot come in. If the entrance record over the ticket from the station near [station / which actually came in] the purpose station will forge supposing it can get the certification equipment holding the ticket with which it is the phase where of entrance was refused and the internal state was rewritten, although entrance with the ticket which is not just cannot be performed in fact, it is showing a ticket with the entrance record forged at the time of participation, and a cheating-on-the-fare action will become possible.

[0025] Thus, when a user chooses himself the ticket which it is going to prove, verification equipment needs to check that the shown ticket can verify justly with the verification equipment, before creating the authorization information which changes an internal state.

[0026] However, in a previous related technique, in order that such a check might not accomplish, there was a trouble that rewrote the internal state corresponding to the ticket which a user does not mean

accidentally, or the injustice by rewriting an internal state was possible.
[0027]
[Problem(s) to be Solved by the Invention] It aims at realizing an electronic ticket system by which verifying and verifying only the ticket which can verify verification equipment does not generate the information to which modification of an internal state is permitted to the ticket which is not right in this invention in order to solve the above-mentioned problem.
[0028]
[Means for Solving the Problem] In order to solve the above-mentioned technical problem, the electronic ticket system concerning this invention It consists of ticket verification equipment and certification equipment. Ticket verification equipment A ticket judging means to judge whether the ticket to verify can verify with verification equipment based on the ticket judging information which certification equipment presents, It has a dialogue verification means to verify whether certification equipment has computed ticket confidential information. Certification equipment It has at least the certification equipment proper information maintenance means, the ticket maintenance means, and a dialogue certification means by which the knowledge about ticket confidential information can be proved, from certification equipment proper information and a ticket.
[0029] In this configuration, verification equipment can check the compatibility of the ticket in certification equipment based on ticket judging information, and only when a right ticket is shown, the internal state of certification equipment can be changed.
[0030]
[The mode of implementation of invention] Hereafter, this invention is explained to a detail.
[0031] The electronic ticket structure-of-a-system Fig. of the example 1 of this invention is shown in [example 1] drawing 2 . In drawing 2 , the electronic ticket system shown in this example consists of verification equipment (it is also called a verification machine) 100, certification equipment (it is also called a certification machine) 200, and ticket assignment equipment 300.
[0032] Verification equipment 100 is constituted including the ticket judging section 101 which judges the justification of the ticket to verify, the authentication information generation section 102, the certification information generation section 103, the certification information verification section 104, the verification equipment privilege information attaching part 105, and the communications department 106.
[0033] On the other hand, certification equipment 200 is constituted including the certification equipment proper information attaching part 201, the ticket attaching part 202, the ticket judging information generation section 203, the authentication information generation section 204, the certification information verification section 205, the certification information generation section 206, the internal-state control section 207, and the communications department 208. In addition, the certification information generation section 103 of verification equipment 100 and the certification information generation section 206 of authentication equipment 200 possess the storage section holding the authentication information sent from authentication equipment 200 and verification equipment 100, respectively.
[0034] Moreover, a ticket and the ticket use information corresponding to each ticket are saved at the ticket attaching part 202. Moreover, the internal-state storage region corresponding to each ticket is secured to the ticket attaching part 202.
[0035] Here, certification equipment 200 is constituted by medium like an IC card with it difficult [to observe internal data and processing procedure from the outside].
[0036] Moreover, in this example, Ticket t is published as follows.
[0037]
[Table 1]
Ticket: t=D-F (n, L, du)
D: the confidential information n:ticket method of a ticket private key du:certification equipment proper -- several F:un-colliding nature one-way function L:ticket use information, however ED**1mod n -- it is E:ticket public key here. Ticket confidential information is D and ticket public information is E, n, and

L. F is realizable with a general Hash Function. Moreover, the information on the conditions using the ticket, for example, an expiration date, the location which can receive service goes into the ticket use information L.

[0038] The outline of the Challenge Handshake Authentication Protocol of this invention is shown in drawing 3 . First, after a user specifies the ticket to be used from now on as certification equipment 200 with ticket assignment equipment 300, Challenge Handshake Authentication Protocol is started between verification equipment 100 and certification equipment 200.

[0039] In drawing 3 , by Challenge Handshake Authentication Protocol, first, the authentication information generation section 102 of verification equipment 100 generates a random number C as authentication information, and sends to certification equipment 200 (S31, S32).

[0040] The certification equipment 200 which received authentication information performs ticket certification information generation processing (S33).

[0041] The flow chart of ticket certification information generation processing (S33) is shown in drawing 4 . In drawing 4 , the certification information generation section 206 of certification equipment 200 computes first the private key D used for a signature by the following count from the certification equipment proper information du saved at Ticket t, the ticket use information L, and the certification equipment proper information attaching part 201 (S41).

[0042]

[Equation 7]

t+F(n,L,du)

=D-F(n,L,du)+F(n,L,du)

= Generate the ticket judging information M to show that D, next the ticket judging information generation section 203 hold the right ticket from the ticket use information on the ticket attaching part 202, and the information on an internal-state storage region (S42). The certification information generation section 206 connects the ticket judging information M with the low order of the bit string of the authentication information C (S43), and is the ticket certification information T [0043]

[Equation 8] T=(C||M) D mod Count of n generates (in addition, S44 and connecting notation || with a bit string are shown). In addition, besides the above-mentioned count, it is [0044].

[Equation 9]

T=(C||M) t(C||M) F (n, L, du) mod The certification information T may be calculated by n.

[0045] Moreover, the authentication information generation section 204 generates a random number chi, and is taken as the 2nd authentication information (S44).

[0046] The ticket certification information T and the 2nd authentication information chi are sent to verification equipment 100 by the communications department 208 (S34). Ticket certification information is a right thing and it signs for guaranteeing that certification equipment and ticket judging information are not forged.

[0047] The verification equipment 100 which received T and chi performs ticket judging processing (S35 of drawing 3).

[0048] The flow chart of ticket judging processing (S35 of drawing 3) is shown in drawing 5 . It is

[0049] from the ticket certification information T that the certification information verification section 104 of verification equipment 100 was sent in drawing 5 , and the ticket public information E which the certification information verification section holds.

[Equation 10] TE mod The value of n is calculated and it checks whether the part of the high order bit connected among the bit string is in agreement with the authentication information C (S51). When in agreement, the ticket judging information M is extracted further (S52). Next, the ticket judging section 101 judges whether it is what the internal state related with the ticket and the ticket based on the contents of M may verify with this verification equipment (S53). When this ticket may be verified as a result of a judgment, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200, and connects it with the low order of chi (S54, S55). Furthermore, the value rho which signed using the confidential information delta showing the privilege of verification equipment is created to this value (S56). Created rho is sent to

certification equipment 200 by the communications department 106 (S36).
[0050] On the other hand, when ticket certification information is not a right thing, or in being what a ticket should not verify, it ends a protocol (S57).
[0051] Next, the certification equipment which received rho performs internal-state modification processing (S37 of drawing 3).
[0052] The flow chart of internal-state modification processing (S37 of drawing 3) is shown in drawing 6 . To the 2nd certification information rho that the certification information verification section 205 of certification equipment 200 was sent in drawing 6 , the public information epsilon which checks the privilege of the verification equipment 100 which self holds is used, and it is [0053].
[Equation 11]
$\rho^{\varepsilon} \mod \nu$

It calculates and checks whether the part of a high order is in agreement with the 2nd authentication information chi among the bit string (S61). As a result of a check, when it becomes clear that it is not right, a protocol is ended to a case (S62). Connected mu is extracted when it is able to be checked that it is a right thing (S63). The internal-state control section 207 changes the internal state of certification equipment 200 according to the contents of mu, and makes the result M' (S64, S65). The certification information generation section 206 is [0054] after connecting the value of M' with the bit string of the authentication information C.
[Equation 12] R=(C||M') D mod Count of n generates the certification information R (S66, S67). R is sent to verification equipment 100 by the communications department 208 (S38).
[0055] The verification equipment 100 which received R performs certification information verification processing (S39 of drawing 3).
[0056] The flow chart of certification information verification processing (S39 of drawing 3) is shown in drawing 7 . The ticket public information E which the certification information verification section 104 of verification equipment 100 holds in drawing 7 is used, and it is [0057].
[Equation 13] RE mod The value of n is calculated and the bit string of the high order except M' connected as a result checks that it is in agreement with the authentication information C which verification equipment 100 generated first (S71). The defined service is offered, when it checks whether the contents of information M' which expresses the modification result of an internal state further are in agreement with the information mu to which internal-state modification sent as 2nd certification information rho is permitted when it is able to check (S72, S73, S74) and a check is completed (S75). When one of checks goes wrong, a protocol is completed and offer of service is not performed (S71, S74, S76).
[0058] The example 2 of [example 2] this invention is the case where an example 1 is realized as a ticket of the ticket of a railroad. The protocol at the time of entrance of a ticket is explained especially here.
[0059] Although the configuration of the example of this invention and the generation method of a ticket are the same as that of an example 1, verification equipment 100 is specifically an automatic ticket gate, and certification equipment 200 is a token like an IC card which can hold a ticket. And verification according to an automatic wicket in entrance and participation shall be performed, and the storage region corresponding to entrance or participation shall be secured to an internal state.
[0060] Below, the example of the ticket on Yokohama - Narita Airport July 18, 1997 explains. In addition, the step to which drawing 3 corresponds is pointed out suitably.
[0061] The ticket use information L on a ticket becomes like drawing 9 . The ticket is registered into certification equipment 200 and the corresponding internal-state storage region is secured. The internal state before entrance is shown in drawing 8 . Here, Ticket ID shows the ticket to be used from now on to 00005.
[0062] First, the authentication at the time of entrance is explained. Verification equipment 100 sends the information showing being entrance to certification equipment 200 with the authentication information C first (S32).
[0063] Certification equipment 200 generates the ticket judging information M. The contents of M are

shown in drawing 10 . As shown in drawing, the contents included in ticket use information and the contents of entrance / participation record of an internal state to show a busy condition are included in the ticket judging information M. The certification information generation section 206 connects M with C, performs the signature by the ticket private key D, and sends it to verification equipment 100 with the 2nd generated authentication information chi as ticket certification information T (S34).

[0064] Verification equipment 100 verifies ticket certification information, and checks the contents of the ticket judging information M further. Here, since an entrance station is within an expiration date and is an intact ticket at the Yokohama station, it is judged with it being the ticket which may carry out authentication here (S35).

[0065] Then, the information mu for changing the internal state of certification equipment 200 is created. The contents of mu are shown in drawing 11 . An entrance name of the station and time amount are recorded on mu. The certification information generation section 103 connects with the 2nd authentication information chi mu generated in this way, generates the value rho which performed the signature using the privilege information delta on verification equipment 100, and sends it to certification equipment 200 (S36).

[0066] The value of rho to which the certification information verification section 205 of certification equipment 200 was sent checks whether it is in agreement with the authentication information chi. When it is able to be checked that it is a right thing, the internal-state control section 207 changes the internal state of certification equipment 200 according to the contents of mu (S37). The situation of the internal state after modification is shown in drawing 12 . It turns out that the station and time amount of entrance were recorded. Next, the internal-state control section 207 makes M' the contents of modification of this internal state, i.e., entrance record. Like an example 1, the certification information generation section 206 connects the value of M' with the bit string of authentication information, generates the value R which performed the signature by ticket confidential information, and sends it to verification equipment 100 as certification information R (S38).

[0067] When the value of the certification information R is verified and the value is in agreement with the authentication information C, verification equipment 100 checks M', as a result of changing an internal state further. If M' corresponds with what was specified by mu, it will be judged as that by which the internal state was changed correctly, and the gate of a ticket gate machine will be opened.

[0068] Next, the authentication at the time of participation is explained. Although the authentication at the time of participation is the same as that of the time of entrance almost, the contents of the message told mutually differ.

[0069] Verification equipment 100 sends the information showing being participation to certification equipment with the authentication information C first (S32).

[0070] The ticket judging information generation section 203 of certification equipment 200 generates the ticket judging information M. The contents of M at the time of participation are shown in drawing 13 . The certification information generation section 206 connects M with C, performs the signature by the ticket private key D, and is taken as the ticket certification information T. And the 2nd authentication information chi which carried out authentication information generation section generation with the certification information T is sent to verification equipment (S34).

[0071] The certification information verification section 104 of verification equipment 100 verifies ticket certification information. In a verification result [of a ticket], or right case, the ticket judging section 101 checks the contents of the ticket judging information M. Here, since an entrance station is effective entrance record and is within the shelf-life of participation at the Yokohama station, it is judged with it being the ticket which can attest participation here (S35).

[0072] Next, the certification information generation section 103 creates the information mu for changing the internal state of certification equipment 200. The contents of mu are shown in drawing 14 . A participation name of the station and participation time amount are recorded on mu. The certification information generation section 103 connects generated mu with chi further, and generates the value rho which performed the signature using the privilege information delta on verification equipment. rho is sent to certification equipment 200 (S36).

[0073] The value of rho to which the certification information verification section 205 of certification equipment 200 was sent checks whether it is in agreement with the authentication information chi. When the right thing is able to be checked, according to the contents of mu, the internal-state control section 207 changes the internal state of certification equipment 200, and makes it M' as a result of [this] modification (i.e., participation record). The situation of the internal state after modification is shown in drawing 15 . A participation station and time amount are recorded. The certification information generation section 206 connects participation record M' with the bit string of the authentication information C, generates the certification information R which performed the signature by ticket confidential information, and sends it to verification equipment 100 (S38).
[0074] When the value of R is verified and the value is in agreement with the authentication information C, the certification information verification section 104 of verification equipment 200 checks M', as a result of changing an internal state further. If M' corresponds with what was specified with the value of mu, it will be judged as that by which the internal state was changed correctly, participation will be permitted, and the gate of a ticket gate machine will be opened (S39).
[0075] The [example 3] example 3 shows how to realize a gestalt like a coupon ticket.
[0076] Fundamentally, the configuration of this example, the generation method of a ticket, and the flow of the whole processing are the same as that of an example 1. The configuration of whole this example is shown in drawing 16 . It differs in that counter 202a which shows the remaining frequency of a coupon ticket is installed in the internal state as a description of this example. In drawing 16 , the sign corresponding to drawing 2 and a corresponding part was attached.
[0077] A user will register with certification equipment 200 first, if a coupon ticket is purchased. The internal-state storage region corresponding to a coupon ticket is secured at the time of registration, and the remaining use counts are written in counter 202a in it.
[0078] After a user specifies a coupon ticket with ticket assignment equipment 300 as a ticket used to certification equipment 200 after this, Challenge Handshake Authentication Protocol is started by the utilization time of a coupon ticket between verification equipment 100 and certification equipment 200.
[0079] At Challenge Handshake Authentication Protocol, it is the same as that of an example 1 till the place where verification equipment 100 generates a random number C as authentication information at, and delivery and certification equipment 200 calculate a ticket private key to certification equipment 200.
[0080] The flow chart of ticket certification information generation processing (it corresponds to S33 of drawing 3) of this example is shown in drawing 17 . In drawing 17 , the ticket judging information generation section 203 of certification equipment 200 extracts the count of the remainder of the internal state corresponding to the ticket of this coupon ticket, and records it on the ticket judging information M with ticket use information (S81-S84). And like an example 1, the certification information generation section 206 generates the ticket certification information T (S85), and the authentication information generation section 204 generates the 2nd authentication information chi (S86). T and chi are sent to verification equipment 100 by the communications department 208 (S34).
[0081] The verification equipment 100 which received T and chi performs ticket judging processing (it is ****** to S35 of drawing 3).
[0082] The flow chart of ticket judging processing is shown in drawing 18 . In drawing 18 , the certification information verification section 104 of verification equipment 100 verifies the received ticket certification information (S91). Ticket certification information extracts the ticket judging information M from ticket certification information to a right case (S92). The count of the remainder of a coupon ticket is recorded on the ticket judging information M. With [that value] one [or more], the ticket judging section 101 judges that this coupon ticket is still usable (S93). Furthermore, when the ticket judging section 101 also judges [that it is verifiable with this verification equipment 100 and] the contents of the ticket use information L, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200 (S94, S95). The contents which direct to reduce the use count of a coupon ticket by one as contents of mu are included. And by the same approach as an example 1, the 2nd certification information rho is created

using mu (S96, S97), and it sends to certification equipment 200 (S36).
[0083] Error processing is performed when verification and a ticket judging go wrong (S98).
[0084] The certification equipment 200 which received rho performs internal-state modification processing (it corresponds to S37 of drawing 3).
[0085] The flow chart of internal-state modification processing is shown in drawing 19 . In drawing 19 , the certification information verification section 205 of certification equipment 200 verifies the 2nd sent certification information rho (S101). When it is able to be checked that it is a right thing, according to the contents of mu, an internal-state control section reduces the remaining use count of a coupon ticket by one, and makes the result M' (S102-S104). The rest is the same approach as an example 1, and certification equipment 200 generates the certification information R, and sends it to verification equipment 100 (S105, S106). Error processing is performed when verification goes wrong at step S101 (S107).
[0086] Actuation of the subsequent verification equipments 100 is the same as that of an example 1, verifies the value of R and offers service.
[0087] In the example 4 of [example 4] this invention, although the whole configuration is the same as that of an example 1, the authentication approaches of ticket public information and ticket confidential information, or a ticket differ.
[0088] this example -- p -- the prime factor -- it is -- G -- dispersion -- a logarithm -- a finite group with a difficult problem -- it is -- g -- the origin of the order p of a finite group G -- it is -- [0089]
[Equation 14] y=gx mod When p is filled, (p, G, g, y) are ticket public information, and make x ticket confidential information. (p, G, g) can also be made common by the whole system.
[0090] At this time, a ticket is [0091] from the ticket description information x, the certification equipment proper information du, the ticket use information L, and the information p that specifies a group.
[Equation 15] t=x-F(du,L,y,p)
It is calculated by carrying out. Here, F is the one-way function of un-colliding nature, and a general Hash Function can realize it. L is the same ticket use information as an example 1.
[0092] Moreover, the above (p, G, g) is [0093] as common as a thing showing the privilege of verification equipment.
[Equation 16]
$\eta = g^{\xi} \mod p$

******** -- let eta [like] into public information and let xi be confidential information.
[0094] G can be constituted as a multiplicative group in fact, or it can constitute as an elliptic curve on finite field.
[0095] The outline of the Challenge Handshake Authentication Protocol of this invention is shown in drawing 20 .
[0096] First, after a user specifies the ticket to be used from now on to certification equipment, Challenge Handshake Authentication Protocol is started between verification equipment and certification equipment.
[0097] In drawing 20 , by this Challenge Handshake Authentication Protocol, first, the authentication information generation section 102 of verification equipment 100 generates a random number r, calculates C=gr, and sends to certification equipment by making this into authentication information (S201, S202, S203).
[0098] The certification equipment 200 which received the authentication information C performs ticket certification information generation processing (S204).
[0099] The flow chart of ticket certification information generation processing is shown in drawing 21 . In drawing 21 , the certification information generation section 206 of certification equipment 200 computes first the private key x used for a signature by the following count from p of Ticket t, the ticket use information L, and ticket public information, and the certification equipment proper information du (S211).

[0100]
[Equation 17]
t+F(y,L,du,p)
=x-F(y,L,du,p)+F(y,L,du,p)
= Generate the ticket judging information M to show that x, next the ticket judging information generation section 203 hold the right ticket from the additional information L of a ticket, and the information on an internal state (S212). The certification information generation section 206 generates the following values as certification information (S213, S214).
[0101]
[Equation 18] T= (C||M) and Cx mod p -- in addition, the certification information T is calculable with the following formulas besides the above.
[0102]
[Equation 19]
T= (C||M) and CtCF (y, L, du, p) mod p and the authentication information generation section 204 generate random-number r' to coincidence, and are [0103].
[Equation 20] Chi=gr' mod p is sent to verification equipment as 2nd authentication information (S215, S216, S205). The information included in the ticket judging information M is the same as that of examples 1-3.
[0104] The certification information T and the 2nd authentication information chi are sent to verification equipment 100 by the communications department 208.
[0105] The verification equipment 100 which received T and chi performs ticket judging processing (S206 of drawing 20).
[0106] The flow chart of ticket judging processing is shown in drawing 22 . It is [0107] from the ticket certification information that the certification information verification section 103 of verification equipment 100 was sent in drawing 22 .
[Equation 21] T/yr mod p= (C||M) and Cx/yr mod The value of p is calculated and it checks whether parts other than M connected among the bit string are in agreement with the authentication information C (S221). When in agreement, the ticket judging section 101 judges further whether it is what the internal state related with the ticket and the ticket may verify with this verification equipment 100 from the contents of the ticket judging information M (S222, S223). When this ticket may be verified as a result of a judgment, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200, and connects it with chi (S224, S225). And the following values are generated as 2nd authentication information to this value using the confidential information xi showing the privilege of verification equipment (S226).
[0108]
[Equation 22]
$$\rho = (\chi \,||\, \mu) \cdot \chi^{F} \mod p$$

rho is sent to certification equipment 200 by the communications department 106. On the other hand, when ticket certification information is not a right thing, or in being what a ticket should not verify, it ends a protocol (S227).
[0109] Next, the certification equipment 200 which received rho performs internal-state modification processing (S208 of drawing 20).
[0110] The flow chart of internal-state modification processing is shown in drawing 23 . It is [0111] from a response indication to which the certification information verification section 205 of certification equipment 200 was sent in drawing 23 .
[Equation 23]
$$\rho / \eta^{r'} \mod p = (\chi \,||\, \mu) \cdot \chi^{F} / \eta^{r'} \mod p$$

A ** value is calculated and it checks whether parts other than mu connected among the bit string are in agreement with the 2nd authentication information chi (S231). When it is able to be checked that it is a

right thing, according to the information the internal-state control section 207 instructs modification of the internal state of mu to be, the internal state of certification equipment 200 changes and the result is made into M' (S232-S234). On the other hand, as a result of a check, when it becomes clear that it is not right, a protocol is ended to a case (S137).
[0112] after the certification information generation section 206 connects the value of M' with the bit string of the authentication information C -- the following values -- certification information -- ** -- it generates by carrying out (S235, S236).
[0113]
[Equation 24] R= (C||M') and Cx mod p -- the certification information R generated in this way is sent to verification equipment 100 by the communications department 208 (S209).
[0114] The verification equipment 100 which received R performs certification information verification processing S210 (drawing 20).
[0115] The flow chart of certification information verification processing is shown in drawing 24 . It is
[0116] from the ticket certification information that the certification information verification section 104 was sent in drawing 24 .
[Equation 25] R/yr mod The value of p= (C||M') and Cx/yrr mod p is calculated and, as a result, the bit string of the high order except M' checks that it is in agreement with the authentication information C which verification equipment 100 generated first (S241). The defined service is offered, when it checks whether the contents of information M' which expresses the modification result of an internal state further are in agreement with the information mu to which internal-state modification sent as 2nd certification information rho is permitted when it is able to check (S242, S243, S244) and a check is completed (S245). When one of checks goes wrong, a protocol is completed and offer of service is not performed (S246).
[0117]
[Effect of the Invention] As explained above, according to this invention, an electronic ticket system by which verifying and verifying only the ticket which can verify verification equipment does not generate the information to which modification of an internal state is permitted to the ticket which is not right can be realized, and the malfeasance by modification of the internal state which a user does not mean, and modification of an internal state can be prevented.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It is the electronic ticket system which has certification equipment and verification equipment and verifies owning the ticket with the above-mentioned just certification equipment. The above-mentioned certification equipment A certification equipment proper information maintenance means to hold the proper information on the above-mentioned certification equipment, and a ticket maintenance means to hold the above-mentioned ticket, The ticket judging information generation section which generates the ticket judging information that the contents of a right of the above-mentioned ticket or the busy condition of the above-mentioned ticket is expressed, Ticket confidential information is generated from the above-mentioned certification equipment proper information and the above-mentioned ticket at least. It has a certification information generation means to generate certification information using the above-mentioned ticket confidential information. The above-mentioned verification equipment A ticket judging means to judge whether I may perform verification processing based on the above-mentioned ticket judging information which the above-mentioned certification equipment presents, The electronic ticket system characterized by having a certification information verification means to verify whether the above-mentioned certification equipment has generated ticket confidential information based on the above-mentioned certification information.
[Claim 2] It is the electronic ticket system are an electronic ticket system according to claim 1, the above-mentioned verification equipment has an authentication information generation means to generate the authentication information used by dialogue certification, and the certification information generation means of the above-mentioned certification equipment generates the above-mentioned certification information using the authentication information which the above-mentioned verification equipment generated.
[Claim 3] It is the electronic ticket system which transmits the ticket judging information on a ticket that it is an electronic ticket system according to claim 2, and the above-mentioned certification equipment and the above-mentioned verification equipment have means of communications, and it is going to prove the above-mentioned certification equipment to the above-mentioned verification equipment.
[Claim 4] They are claim 2 thru/or an electronic ticket system given in 3. The above-mentioned electronic ticket system The above-mentioned verification equipment and the above-mentioned certification equipment are resembled, in addition it has ticket issue equipment. The above-mentioned ticket issue equipment A ticket description information maintenance means to hold the above-mentioned ticket confidential information which is the secret description information on the ticket to publish, and corresponding ticket public information, A certification equipment proper information maintenance means for ticket issue to hold the proper information on the above-mentioned certification equipment which a user holds, The electronic ticket system which has ticket issue ****** which creates the ticket which is digital information using the above-mentioned ticket confidential information currently held for the above-mentioned ticket description information maintenance means, and the above-mentioned certification equipment proper information currently held for the above-mentioned certification equipment proper information maintenance means for ticket issue.

[Claim 5] It is the electronic ticket system are claim 2 thru/or the electronic ticket system of 4, and the certification information generation means of the above-mentioned certification equipment is a predetermined approach, and calculates the ticket certification information use to the judgment of the above-mentioned ticket judging means as one of the above-mentioned certification information, from the authentication information sent from the above-mentioned verification equipment at least, the above-mentioned ticket, the above-mentioned ticket judging information, and the above-mentioned certification equipment proper information.
[Claim 6] It is the electronic ticket system which are an electronic ticket system according to claim 5, and the above-mentioned certification equipment makes the ticket use information that the use conditions of a ticket were defined correspond with a ticket, and holds to the above-mentioned ticket attaching part.
[Claim 7] It is the electronic ticket system which uses the above-mentioned ticket use information at least in case it is an electronic ticket system according to claim 5 and the above-mentioned certification equipment creates the above-mentioned ticket judging information.
[Claim 8] It is the electronic ticket system which is an electronic ticket system according to claim 6, and is equipped with the internal-state storage region holding a strange internal state with the above-mentioned good certification equipment, and the internal-state control means which controls the value of the above-mentioned internal state.
[Claim 9] It is the electronic ticket system which uses the information on the internal-state storage region of the above-mentioned certification equipment at least in case it is an electronic ticket system according to claim 8 and the ticket judging information generation means of the above-mentioned certification equipment creates the above-mentioned ticket judging information.
[Claim 10] It rewrites from the outside and at least the part of the strange good internal states which are claim 8 thru/or the electronic ticket system of 9, and the internal-state storage region of the above-mentioned certification equipment holds is a impossible electronic ticket system.
[Claim 11] It is the electronic ticket system by which it is claim 8 thru/or the electronic ticket system of 10, and the certification information generation means of the above-mentioned certification equipment calculates the above-mentioned certification information at least using the above-mentioned ticket, the above-mentioned ticket use information, and the above-mentioned certification equipment proper information.
[Claim 12] It is the electronic ticket system are claim 8 thru/or the electronic ticket system of 11, and above-mentioned certification equipment has the authentication information maintenance means hold the above-mentioned authentication information sent from the above-mentioned verification means, and the above-mentioned certification information generation means changes the authentication information currently held at the above-mentioned authentication information maintenance means using the ticket judging information generated by the above-mentioned ticket judging information generation means, and use to generation of the above-mentioned certification information.
[Claim 13] When ticket judging information which is the electronic ticket system of claim 12 and the above-mentioned ticket judging information generation means generated is set to M and the above-mentioned authentication information sets to C, the certification information generation means of the above-mentioned certification equipment is the electronic ticket system which updates to what joined M to C in the authentication information C currently held at the above-mentioned authentication information maintenance means.
[Claim 14] They are claim 12 thru/or the electronic ticket system of 13. The certification information generation means of the above-mentioned certification equipment It is possible to generate ticket certification information as one of the above-mentioned certification information. The above-mentioned ticket certification information The electronic ticket system generated by calculating ticket confidential information by the predetermined approach from the above-mentioned ticket, the above-mentioned ticket use information, and the above-mentioned certification equipment proper information, and performing count using ticket confidential information to the above-mentioned authentication information.

[Claim 15] It is the electronic ticket system of claim 14, p and q are the prime factors, and it is n=p-q, and is DE**1. mod (p-1) (q-1) When relation is filled, The above-mentioned ticket confidential information is D, ticket public information is (n, E), the above-mentioned ticket use information is L, the above-mentioned certification equipment proper information is the secret value du, and, on the other hand, f (du, L, n) is made into a tropism function. When the ticket is given by t=D-f (du, L, n), the certification information generation means of the above-mentioned certification equipment As opposed to the above-mentioned authentication information C (authentication information which the above-mentioned certification information generation means changed) the law of C -- the power by t in n, and the law of C -- law with the power in n according to the tropism function value f (du, L, n) on the other hand -- product CtCf in n (du, L, n) mod Electronic ticket system which calculates ticket certification information as n.

[Claim 16] It is the electronic ticket system of claim 14, p and q are the prime factors, and it is n=p-q, and is DE**1. mod (p-1) (q-1) When relation is filled, The above-mentioned ticket confidential information is D, ticket public information is (n, E), the above-mentioned ticket use information is L, the above-mentioned certification equipment proper information is the secret value du, and, on the other hand, f (du, L, n) is made into a tropism function. When the above-mentioned ticket is given by t=D-f (du, L, n), the above-mentioned certification equipment t+f(du, L, n) =D is calculated beforehand, the value is used, and it is T=CD to the above-mentioned authentication information C (authentication information which the above-mentioned certification information generation means changed). mod Electronic ticket system which calculates the ticket certification information T as n.

[Claim 17] the electronic ticket system of claim 14 -- it is -- g -- dispersion -- a logarithm -- the primitive root of a group with a difficult problem -- it is -- p -- the prime factor -- it is -- an integer x -- receiving -- y=gxmod When p is realized The above-mentioned ticket confidential information is x, ticket public information is (y, p, g), the above-mentioned ticket use information is L, the above-mentioned certification equipment proper information is the secret value du, and, on the other hand, f (du, L, y) is made into a tropism function. When the above-mentioned ticket is given by t=x-f (du, L, y), the above-mentioned certification equipment As opposed to the above-mentioned authentication information C (authentication information which the above-mentioned certification information generation means changed) the above-mentioned ticket judging information T -- the law of C -- the power by t in p, and the law of C -- law with the power in p which, on the other hand, makes a characteristic the tropism function value f (du, L, y) -- product CtCf in p (du, L, y) Electronic ticket system which calculates the above-mentioned certification information as modn.

[Claim 18] the electronic ticket system of claim 14 -- it is -- g -- dispersion -- a logarithm -- the primitive root of a group with a difficult problem -- it is -- p -- the prime factor -- it is -- an integer x -- receiving -- y=gxmod When p is realized The above-mentioned ticket confidential information is x, ticket public information is (y, p, g), the above-mentioned ticket use information is L, the above-mentioned certification equipment proper information is the secret value du, and, on the other hand, f (du, L, y) is made into a tropism function. When the above-mentioned ticket is given by t=x-f (du, L, y), the above-mentioned certification equipment It is Cx, in case t+f(du, L, y) =x are calculated beforehand and the ticket (authentication information which above-mentioned certification information generation means changed) judging information T is calculated to the above-mentioned authentication information C. mod Electronic ticket system using the value of p.

[Claim 19] It is the electronic ticket system are claim 14 thru/or the electronic ticket system of 18, and the certification information verification means of the above-mentioned verification equipment verifies the justification of the above-mentioned ticket certification information from the authentication information which the above-mentioned authentication information generation means created, the ticket certification information which were sent from the above-mentioned certification equipment, and the above-mentioned ticket public information, and a right case derives the ticket judging information were embedded to the above-mentioned ticket certification information, in the above-mentioned ticket certification information.

[Claim 20] It is the electronic ticket system of claim 19, and the above-mentioned authentication

information is C. When the above-mentioned ticket certification information is T, it is the above-mentioned ticket public information (n, E) and there is certain bit string M, the certification information verification means of the above-mentioned verification equipment the above-mentioned ticket certification information T -- law -- the bit string which joined C and M for what carried out the exponentiation by E by n -- comparing -- TE mod If it is n=C||M (notation || is junction of a bit string) It is the electronic ticket system by which the above-mentioned ticket certification information is judged to be the right, and the above-mentioned ticket certification information derives M as the above-mentioned ticket judging information in a right case.

[Claim 21] It is the electronic ticket system of claim 19, and the above-mentioned authentication information is C. When the above-mentioned ticket certification information is T and the above-mentioned ticket public information is (p, g, y), the certification information verification means of the above-mentioned verification equipment When setting to r the random number which self generated, there is certain bit string M, and it is T/yr. mod p= (C||M) (notation || is junction of a bit string) If it has become It is the electronic ticket system by which the above-mentioned ticket certification information is judged to be the right, and the above-mentioned ticket certification information derives M as ticket judging information in a right case.

[Claim 22] They are claim 8 thru/or the electronic ticket system of 21. The above-mentioned certification equipment 2nd authentication information generation means to generate the 2nd authentication information for attesting the above-mentioned verification equipment, It has the 2nd certification information verification means for verifying the 2nd certification information which the above-mentioned verification equipment generates. The certification information verification means of the above 2nd The certification information on the above 2nd is the electronic ticket system by which the certification information on the above 2nd verifies whether it is the right from the authentication information on the above 2nd, the certification information on the above 2nd, and ticket public information, and the above-mentioned internal-state control means changes the internal state of the above-mentioned certification equipment a right case.

[Claim 23] It is the electronic ticket system which determines whether are the electronic ticket system of claim 22 and the certification information verification means of the above-mentioned verification equipment generates the certification information on the above 2nd based on the result of the judgment by the above-mentioned ticket judging means.

[Claim 24] It is the electronic ticket system which it is the electronic ticket system of claim 22, and the above-mentioned certification equipment relates with a ticket the internal state which functions as a counter of a ticket, holds from the exterior to an internal-state storage region in the form which is not rewritable, and judges the certification information verification means of the above-mentioned verification equipment to be what has a corresponding ticket invalid when the value of the counter of the internal state included in the ticket judging information sent from the above-mentioned certification equipment is a predetermined value.

[Claim 25] It is claim 22 thru/or the electronic ticket system of 24, p' and q' are the prime factors, and it is nu=p'-q', and is deltaepsilon**1. mod (p' - 1) (q' - 1) When relation is filled, for the 2nd certification information verification means of the above-mentioned certification equipment, the authentication information chi on the above 2nd and the certification information rho on the above 2nd are [Equation 1].

$$\chi = \rho^{\varepsilon} \mod \nu$$

The electronic ticket system which the certification information on the above 2nd judges to a ******** case to be the right.

[Claim 26] claim 22 thru/or the electronic ticket system of 24 -- it is -- g -- dispersion -- a logarithm -- the primitive root of a group with a difficult problem -- it is -- p -- the prime factor -- it is -- an integer xi -- receiving -- [Equation 2]

$$\eta = g^{\xi} \mod p$$

******** -- suddenly -- coming -- alike -- the 2nd authentication information generation means of certification equipment -- random-number r' and authentication information chi=gr' of the above 2nd -- generating -- the certification information verification means of the above 2nd -- the certification information rho on the above 2nd -- rho/etar' mod ********** system which the certification information on the above 2nd judges to be the right when p=chi is filled.
[Claim 27] The certification information on the above 2nd is the electronic ticket system by which the information which is the electronic ticket system of claim 22, and as for which the 2nd certification information verification means of the above-mentioned certification equipment was embedded by the right case to the certification information on the above 2nd is derived.
[Claim 28] It is the electronic ticket system which uses as information for being the electronic ticket system of claim 27 and permitting modification of the above-mentioned internal information for the information by which the 2nd certification information verification means of the above-mentioned certification equipment was drawn from the certification information on the above 2nd.
[Claim 29] It is claim 27 thru/or the electronic ticket system of 28, ticket public information contains nu and epsilon, and, for the 2nd certification information verification means of the above-mentioned certification equipment, the authentication information chi on the above 2nd and the certification information rho on the above 2nd are [Equation 3] to certain bit string mu.
$\chi \| \mu = \rho^{\varepsilon} \mod \nu$ (記号||はビット列の接合)

The electronic ticket system by which the certification information on the above 2nd judges with the right, and derives mu as information embedded to the certification information on the above 2nd at the time of ********.
[Claim 30] It is the electronic ticket system which changes the internal state which is the electronic ticket system of claim 27 and was held in the above-mentioned internal-state storage region based on the information by which the internal-state control means of the above-mentioned certification equipment was drawn from the certification information on the above 2nd.
[Claim 31] It is the electronic ticket system which judges whether it is the electronic ticket system of claim 30, and the certification information verification means of the above 2nd of the above-mentioned certification equipment generates the above-mentioned certification information correctly based on the information to which internal-state modification sent from the above-mentioned verification equipment is permitted, and an internal state.
[Claim 32] It is the electronic ticket system are claim 22 thru/or the electronic ticket system of 31, above-mentioned verification equipment has the verification equipment privilege information attaching part holding verification equipment privilege information which is the confidential information showing the privilege of the above-mentioned verification equipment, and the 2nd certification information generation section which generates the certification information on the above 2nd, and the certification information generation section of the above 2nd generates the 2nd certification information from the authentication information on the above 2nd, and above-mentioned verification equipment privilege information.
[Claim 33] When it is the electronic ticket system of claim 32, the above-mentioned verification equipment privilege information is set to delta and corresponding public information is set to (nu, epsilon), the 2nd certification information generation section of the above-mentioned verification equipment is [Equation 4] about the certification information rho on the above 2nd from the authentication information chi on the above 2nd.
$\rho = \chi^{\delta} \mod \nu$

The electronic ticket system which generate by carrying out.
[Claim 34] It is the electronic ticket system of claim 32, and the above-mentioned verification equipment privilege information is set to xi, corresponding public information is set to (p, g, eta), and it is [Equation 5].
$\eta = g^{\xi} \mod p$

The 2nd certification information generation section of the above-mentioned verification equipment is [as opposed to / when ****** is filled / the authentication information chi on the above 2nd] [Equation 6].

$$\chi^{r} \mod p$$

The electronic ticket system which generates the certification information rho on the above 2nd using a ** value.

[Claim 35] It is the electronic ticket system are claim 32 thru/or the electronic ticket system of 34, and the above-mentioned verification equipment has the 2nd authentication information attaching part holding the authentication information on the above 2nd, and calculate the certification information on the above 2nd from the information grant a permission in modification of the internal state of certification equipment, and the authentication information on the above 2nd in case the 2nd certification information generation section of the above-mentioned verification equipment gives the count which used the above-mentioned verification equipment privilege information.

[Claim 36] It is the electronic ticket system which updates the authentication information on the above 2nd held at the authentication information attaching part of the above 2nd using the information to which modification of the internal state of the above-mentioned certification equipment is permitted before it is claim 32 thru/or the electronic ticket system of 34 and the 2nd certification information generation section of the above-mentioned verification equipment performs count which used the above-mentioned verification equipment privilege information.

[Claim 37] It is the electronic ticket system which updates to what was the electronic ticket system of claim 36, and joined mu for the 2nd authentication information held at the authentication information attaching part of the above 2nd at chi when the 2nd certification information generation section of the above-mentioned verification equipment set to mu information to which modification of the internal state of the above-mentioned certification equipment is permitted and authentication information on the above 2nd was set to chi.

[Claim 38] The electronic ticket system currently held in a defense means to be claim 1 thru/or an electronic ticket system given in 37, and to close at least that the above-mentioned certification equipment observes internal data and processing procedure from the outside if .

[Claim 39] The electronic ticket system by which it is a claim thru/or an electronic ticket system given in 37, and the above-mentioned certification equipment is constituted as a portable small arithmetic unit of an IC card etc. at least.

[Claim 40] It is the electronic ticket system which has certification equipment and verification equipment and verifies owning the ticket with the above-mentioned just certification equipment. The above-mentioned certification equipment A certification equipment proper information maintenance means to hold the proper information on the above-mentioned certification equipment, and a ticket maintenance means to hold the above-mentioned ticket, The ticket judging information generation section which generates the ticket judging information that the contents of a right of the above-mentioned ticket or the busy condition of the above-mentioned ticket is expressed, It has a certification information generation means to generate certification information from the above-mentioned certification equipment proper information and the above-mentioned ticket at least. The above-mentioned verification equipment A ticket judging means to judge whether I may perform verification processing based on the above-mentioned ticket judging information which the above-mentioned certification equipment presents, The electronic ticket system by which the above-mentioned certification equipment is characterized by having a certification information verification means to verify whether the above-mentioned certification information was generable from the above-mentioned certification equipment proper information and the above-mentioned ticket.

[Claim 41] In the electronic ticket use approach of performing service predetermined by the verification equipment side, performing mutual recognition between verification equipment and the authentication equipment holding an electronic ticket, and changing an internal state by the authentication equipment

side The step which shows the above-mentioned verification equipment the ticket judging information that the above-mentioned certification equipment expresses the contents of a right of the above-mentioned electronic ticket, or the busy condition of the above-mentioned electronic ticket, The electronic ticket use approach that the above-mentioned verification equipment is characterized by having the step which judges whether I may perform verification processing based on the shown above-mentioned ticket judging information.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention] This invention relates to the technique of creating a ticket and a card electronically and using them.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Background of the Invention]

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] As explained above, according to this invention, an electronic ticket system by which verifying and verifying only the ticket which can verify verification equipment does not generate the information to which modification of an internal state is permitted to the ticket which is not right can be realized, and the malfeasance by modification of the internal state which a user does not mean, and modification of an internal state can be prevented.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] It aims at realizing an electronic ticket system by which verifying and verifying only the ticket which can verify verification equipment does not generate the information to which modification of an internal state is permitted to the ticket which is not right in this invention in order to solve the above-mentioned problem.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] In order to solve the above-mentioned technical problem, the electronic ticket system concerning this invention It consists of ticket verification equipment and certification equipment. Ticket verification equipment A ticket judging means to judge whether the ticket to verify can verify with verification equipment based on the ticket judging information which certification equipment presents, It has a dialogue verification means to verify whether certification equipment has computed ticket confidential information. Certification equipment It has at least the certification equipment proper information maintenance means, the ticket maintenance means, and a dialogue certification means by which the knowledge about ticket confidential information can be proved, from certification equipment proper information and a ticket.
[0029] In this configuration, verification equipment can check the compatibility of the ticket in certification equipment based on ticket judging information, and only when a right ticket is shown, the internal state of certification equipment can be changed.
[0030]
[The mode of implementation of invention] Hereafter, this invention is explained to a detail.
[0031] The electronic ticket structure-of-a-system Fig. of the example 1 of this invention is shown in [example 1] drawing 2 . In drawing 2 , the electronic ticket system shown in this example consists of verification equipment (it is also called a verification machine) 100, certification equipment (it is also called a certification machine) 200, and ticket assignment equipment 300.
[0032] Verification equipment 100 is constituted including the ticket judging section 101 which judges the justification of the ticket to verify, the authentication information generation section 102, the certification information generation section 103, the certification information verification section 104, the verification equipment privilege information attaching part 105, and the communications department 106.
[0033] On the other hand, certification equipment 200 is constituted including the certification equipment proper information attaching part 201, the ticket attaching part 202, the ticket judging information generation section 203, the authentication information generation section 204, the certification information verification section 205, the certification information generation section 206, the internal-state control section 207, and the communications department 208. In addition, the certification information generation section 103 of verification equipment 100 and the certification information generation section 206 of authentication equipment 200 possess the storage section holding the authentication information sent from authentication equipment 200 and verification equipment 100, respectively.
[0034] Moreover, a ticket and the ticket use information corresponding to each ticket are saved at the ticket attaching part 202. Moreover, the internal-state storage region corresponding to each ticket is secured to the ticket attaching part 202.
[0035] Here, certification equipment 200 is constituted by medium like an IC card with it difficult [to observe internal data and processing procedure from the outside].
[0036] Moreover, in this example, Ticket t is published as follows.

[0037]
[Table 1]
Ticket: t=D-F (n, L, du)
D: the confidential information n:ticket method of a ticket private key du:certification equipment proper -- several F:un-colliding nature one-way function L:ticket use information, however ED**1mod n -- it is E:ticket public key here. Ticket confidential information is D and ticket public information is E, n, and L. F is realizable with a general Hash Function. Moreover, the information on the conditions using the ticket, for example, an expiration date, the location which can receive service goes into the ticket use information L.
[0038] The outline of the Challenge Handshake Authentication Protocol of this invention is shown in drawing 3 . First, after a user specifies the ticket to be used from now on as certification equipment 200 with ticket assignment equipment 300, Challenge Handshake Authentication Protocol is started between verification equipment 100 and certification equipment 200.
[0039] In drawing 3 , by Challenge Handshake Authentication Protocol, first, the authentication information generation section 102 of verification equipment 100 generates a random number C as authentication information, and sends to certification equipment 200 (S31, S32).
[0040] The certification equipment 200 which received authentication information performs ticket certification information generation processing (S33).
[0041] The flow chart of ticket certification information generation processing (S33) is shown in drawing 4 . In drawing 4 , the certification information generation section 206 of certification equipment 200 computes first the private key D used for a signature by the following count from the certification equipment proper information du saved at Ticket t, the ticket use information L, and the certification equipment proper information attaching part 201 (S41).
[0042]
[Equation 7]
t+F(n,L,du)
=D-F(n,L,du)+F(n,L,du)
= Generate the ticket judging information M to show that D, next the ticket judging information generation section 203 hold the right ticket from the ticket use information on the ticket attaching part 202, and the information on an internal-state storage region (S42). The certification information generation section 206 connects the ticket judging information M with the low order of the bit string of the authentication information C (S43), and is the ticket certification information T [0043]
[Equation 8] T=(C||M) D mod Count of n generates (in addition, S44 and connecting notation || with a bit string are shown). In addition, besides the above-mentioned count, it is [0044].
[Equation 9]
T=(C||M) t(C||M) F (n, L, du) mod The certification information T may be calculated by n.
[0045] Moreover, the authentication information generation section 204 generates a random number chi, and is taken as the 2nd authentication information (S44).
[0046] The ticket certification information T and the 2nd authentication information chi are sent to verification equipment 100 by the communications department 208 (S34). Ticket certification information is a right thing and it signs for guaranteeing that certification equipment and ticket judging information are not forged.
[0047] The verification equipment 100 which received T and chi performs ticket judging processing (S35 of drawing 3).
[0048] The flow chart of ticket judging processing (S35 of drawing 3) is shown in drawing 5 . It is
[0049] from the ticket certification information T that the certification information verification section 104 of verification equipment 100 was sent in drawing 5 , and the ticket public information E which the certification information verification section holds.
[Equation 10] TE mod The value of n is calculated and it checks whether the part of the high order bit connected among the bit string is in agreement with the authentication information C (S51). When in agreement, the ticket judging information M is extracted further (S52). Next, the ticket judging section

101 judges whether it is what the internal state related with the ticket and the ticket based on the contents of M may verify with this verification equipment (S53). When this ticket may be verified as a result of a judgment, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200, and connects it with the low order of chi (S54, S55). Furthermore, the value rho which signed using the confidential information delta showing the privilege of verification equipment is created to this value (S56). Created rho is sent to certification equipment 200 by the communications department 106 (S36).
[0050] On the other hand, when ticket certification information is not a right thing, or in being what a ticket should not verify, it ends a protocol (S57).
[0051] Next, the certification equipment which received rho performs internal-state modification processing (S37 of drawing 3).
[0052] The flow chart of internal-state modification processing (S37 of drawing 3) is shown in drawing 6 . To the 2nd certification information rho that the certification information verification section 205 of certification equipment 200 was sent in drawing 6 , the public information epsilon which checks the privilege of the verification equipment 100 which self holds is used, and it is [0053].
[Equation 11]
$\rho^{\varepsilon} \mod \nu$

It calculates and checks whether the part of a high order is in agreement with the 2nd authentication information chi among the bit string (S61). As a result of a check, when it becomes clear that it is not right, a protocol is ended to a case (S62). Connected mu is extracted when it is able to be checked that it is a right thing (S63). The internal-state control section 207 changes the internal state of certification equipment 200 according to the contents of mu, and makes the result M' (S64, S65). The certification information generation section 206 is [0054] after connecting the value of M' with the bit string of the authentication information C.
[Equation 12] R=(C||M') D mod Count of n generates the certification information R (S66, S67). R is sent to verification equipment 100 by the communications department 208 (S38).
[0055] The verification equipment 100 which received R performs certification information verification processing (S39 of drawing 3).
[0056] The flow chart of certification information verification processing (S39 of drawing 3) is shown in drawing 7 . The ticket public information E which the certification information verification section 104 of verification equipment 100 holds in drawing 7 is used, and it is [0057].
[Equation 13] RE mod The value of n is calculated and the bit string of the high order except M' connected as a result checks that it is in agreement with the authentication information C which verification equipment 100 generated first (S71). The defined service is offered, when it checks whether the contents of information M' which expresses the modification result of an internal state further are in agreement with the information mu to which internal-state modification sent as 2nd certification information rho is permitted when it is able to check (S72, S73, S74) and a check is completed (S75). When one of checks goes wrong, a protocol is completed and offer of service is not performed (S71, S74, S76).
[0058] The example 2 of [example 2] this invention is the case where an example 1 is realized as a ticket of the ticket of a railroad. The protocol at the time of entrance of a ticket is explained especially here.
[0059] Although the configuration of the example of this invention and the generation method of a ticket are the same as that of an example 1, verification equipment 100 is specifically an automatic ticket gate, and certification equipment 200 is a token like an IC card which can hold a ticket. And verification according to an automatic wicket in entrance and participation shall be performed, and the storage region corresponding to entrance or participation shall be secured to an internal state.
[0060] Below, the example of the ticket on Yokohama - Narita Airport July 18, 1997 explains. In addition, the step to which drawing 3 corresponds is pointed out suitably.
[0061] The ticket use information L on a ticket becomes like drawing 9 . The ticket is registered into certification equipment 200 and the corresponding internal-state storage region is secured. The internal

state before entrance is shown in drawing 8 . Here, Ticket ID shows the ticket to be used from now on to 00005.

[0062] First, the authentication at the time of entrance is explained. Verification equipment 100 sends the information showing being entrance to certification equipment 200 with the authentication information C first (S32).

[0063] Certification equipment 200 generates the ticket judging information M. The contents of M are shown in drawing 10 . As shown in drawing, the contents included in ticket use information and the contents of entrance / participation record of an internal state to show a busy condition are included in the ticket judging information M. The certification information generation section 206 connects M with C, performs the signature by the ticket private key D, and sends it to verification equipment 100 with the 2nd generated authentication information chi as ticket certification information T (S34).

[0064] Verification equipment 100 verifies ticket certification information, and checks the contents of the ticket judging information M further. Here, since an entrance station is within an expiration date and is an intact ticket at the Yokohama station, it is judged with it being the ticket which may carry out authentication here (S35).

[0065] Then, the information mu for changing the internal state of certification equipment 200 is created. The contents of mu are shown in drawing 11 . An entrance name of the station and time amount are recorded on mu. The certification information generation section 103 connects with the 2nd authentication information chi mu generated in this way, generates the value rho which performed the signature using the privilege information delta on verification equipment 100, and sends it to certification equipment 200 (S36).

[0066] The value of rho to which the certification information verification section 205 of certification equipment 200 was sent checks whether it is in agreement with the authentication information chi. When it is able to be checked that it is a right thing, the internal-state control section 207 changes the internal state of certification equipment 200 according to the contents of mu (S37). The situation of the internal state after modification is shown in drawing 12 . It turns out that the station and time amount of entrance were recorded. Next, the internal-state control section 207 makes M' the contents of modification of this internal state, i.e., entrance record. Like an example 1, the certification information generation section 206 connects the value of M' with the bit string of authentication information, generates the value R which performed the signature by ticket confidential information, and sends it to verification equipment 100 as certification information R (S38).

[0067] When the value of the certification information R is verified and the value is in agreement with the authentication information C, verification equipment 100 checks M', as a result of changing an internal state further. If M' corresponds with what was specified by mu, it will be judged as that by which the internal state was changed correctly, and the gate of a ticket gate machine will be opened.

[0068] Next, the authentication at the time of participation is explained. Although the authentication at the time of participation is the same as that of the time of entrance almost, the contents of the message told mutually differ.

[0069] Verification equipment 100 sends the information showing being participation to certification equipment with the authentication information C first (S32).

[0070] The ticket judging information generation section 203 of certification equipment 200 generates the ticket judging information M. The contents of M at the time of participation are shown in drawing 13 . The certification information generation section 206 connects M with C, performs the signature by the ticket private key D, and is taken as the ticket certification information T. And the 2nd authentication information chi which carried out authentication information generation section generation with the certification information T is sent to verification equipment (S34).

[0071] The certification information verification section 104 of verification equipment 100 verifies ticket certification information. In a verification result [of a ticket], or right case, the ticket judging section 101 checks the contents of the ticket judging information M. Here, since an entrance station is effective entrance record and is within the shelf-life of participation at the Yokohama station, it is judged with it being the ticket which can attest participation here (S35).

[0072] Next, the certification information generation section 103 creates the information mu for changing the internal state of certification equipment 200. The contents of mu are shown in drawing 14 . A participation name of the station and participation time amount are recorded on mu. The certification information generation section 103 connects generated mu with chi further, and generates the value rho which performed the signature using the privilege information delta on verification equipment. rho is sent to certification equipment 200 (S36).
[0073] The value of rho to which the certification information verification section 205 of certification equipment 200 was sent checks whether it is in agreement with the authentication information chi. When the right thing is able to be checked, according to the contents of mu, the internal-state control section 207 changes the internal state of certification equipment 200, and makes it M' as a result of [this] modification (i.e., participation record). The situation of the internal state after modification is shown in drawing 15 . A participation station and time amount are recorded. The certification information generation section 206 connects participation record M' with the bit string of the authentication information C, generates the certification information R which performed the signature by ticket confidential information, and sends it to verification equipment 100 (S38).
[0074] When the value of R is verified and the value is in agreement with the authentication information C, the certification information verification section 104 of verification equipment 200 checks M', as a result of changing an internal state further. If M' corresponds with what was specified with the value of mu, it will be judged as that by which the internal state was changed correctly, participation will be permitted, and the gate of a ticket gate machine will be opened (S39).
[0075] The [example 3] example 3 shows how to realize a gestalt like a coupon ticket.
[0076] Fundamentally, the configuration of this example, the generation method of a ticket, and the flow of the whole processing are the same as that of an example 1. The configuration of whole this example is shown in drawing 16 . It differs in that counter 202a which shows the remaining frequency of a coupon ticket is installed in the internal state as a description of this example. In drawing 16 , the sign corresponding to drawing 2 and a corresponding part was attached.
[0077] A user will register with certification equipment 200 first, if a coupon ticket is purchased. The internal-state storage region corresponding to a coupon ticket is secured at the time of registration, and the remaining use counts are written in counter 202a in it.
[0078] After a user specifies a coupon ticket with ticket assignment equipment 300 as a ticket used to certification equipment 200 after this, Challenge Handshake Authentication Protocol is started by the utilization time of a coupon ticket between verification equipment 100 and certification equipment 200.
[0079] At Challenge Handshake Authentication Protocol, it is the same as that of an example 1 till the place where verification equipment 100 generates a random number C as authentication information at, and delivery and certification equipment 200 calculate a ticket private key to certification equipment 200.
[0080] The flow chart of ticket certification information generation processing (it corresponds to S33 of drawing 3) of this example is shown in drawing 17 . In drawing 17 , the ticket judging information generation section 203 of certification equipment 200 extracts the count of the remainder of the internal state corresponding to the ticket of this coupon ticket, and records it on the ticket judging information M with ticket use information (S81-S84). And like an example 1, the certification information generation section 206 generates the ticket certification information T (S85), and the authentication information generation section 204 generates the 2nd authentication information chi (S86). T and chi are sent to verification equipment 100 by the communications department 208 (S34).
[0081] The verification equipment 100 which received T and chi performs ticket judging processing (it is ****** to S35 of drawing 3).
[0082] The flow chart of ticket judging processing is shown in drawing 18 . In drawing 18 , the certification information verification section 104 of verification equipment 100 verifies the received ticket certification information (S91). Ticket certification information extracts the ticket judging information M from ticket certification information to a right case (S92). The count of the remainder of a coupon ticket is recorded on the ticket judging information M. With [that value] one [or more], the

ticket judging section 101 judges that this coupon ticket is still usable (S93). Furthermore, when the ticket judging section 101 also judges [that it is verifiable with this verification equipment 100 and] the contents of the ticket use information L, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200 (S94, S95). The contents which direct to reduce the use count of a coupon ticket by one as contents of mu are included. And by the same approach as an example 1, the 2nd certification information rho is created using mu (S96, S97), and it sends to certification equipment 200 (S36).
[0083] Error processing is performed when verification and a ticket judging go wrong (S98).
[0084] The certification equipment 200 which received rho performs internal-state modification processing (it corresponds to S37 of drawing 3).
[0085] The flow chart of internal-state modification processing is shown in drawing 19 . In drawing 19 , the certification information verification section 205 of certification equipment 200 verifies the 2nd sent certification information rho (S101). When it is able to be checked that it is a right thing, according to the contents of mu, an internal-state control section reduces the remaining use count of a coupon ticket by one, and makes the result M' (S102-S104). The rest is the same approach as an example 1, and certification equipment 200 generates the certification information R, and sends it to verification equipment 100 (S105, S106). Error processing is performed when verification goes wrong at step S101 (S107).
[0086] Actuation of the subsequent verification equipments 100 is the same as that of an example 1, verifies the value of R and offers service.
[0087] In the example 4 of [example 4] this invention, although the whole configuration is the same as that of an example 1, the authentication approaches of ticket public information and ticket confidential information, or a ticket differ.
[0088] this example -- p -- the prime factor -- it is -- G -- dispersion -- a logarithm -- a finite group with a difficult problem -- it is -- g -- the origin of the order p of a finite group G -- it is -- [0089]
[Equation 14] y=gx mod When p is filled, (p, G, g, y) are ticket public information, and make x ticket confidential information. (p, G, g) can also be made common by the whole system.
[0090] At this time, a ticket is [0091] from the ticket description information x, the certification equipment proper information du, the ticket use information L, and the information p that specifies a group.
[Equation 15] t=x-F(du,L,y,p)
It is calculated by carrying out. Here, F is the one-way function of un-colliding nature, and a general Hash Function can realize it. L is the same ticket use information as an example 1.
[0092] Moreover, the above (p, G, g) is [0093] as common as a thing showing the privilege of verification equipment.
[Equation 16]
$$\eta = g^{\xi} \mod p$$

******** -- let eta [like] into public information and let xi be confidential information.
[0094] G can be constituted as a multiplicative group in fact, or it can constitute as an elliptic curve on finite field.
[0095] The outline of the Challenge Handshake Authentication Protocol of this invention is shown in drawing 20 .
[0096] First, after a user specifies the ticket to be used from now on to certification equipment, Challenge Handshake Authentication Protocol is started between verification equipment and certification equipment.
[0097] In drawing 20 , by this Challenge Handshake Authentication Protocol, first, the authentication information generation section 102 of verification equipment 100 generates a random number r, calculates C=gr, and sends to certification equipment by making this into authentication information (S201, S202, S203).
[0098] The certification equipment 200 which received the authentication information C performs ticket

certification information generation processing (S204).
[0099] The flow chart of ticket certification information generation processing is shown in drawing 21 . In drawing 21 , the certification information generation section 206 of certification equipment 200 computes first the private key x used for a signature by the following count from p of Ticket t, the ticket use information L, and ticket public information, and the certification equipment proper information du (S211).
[0100]
[Equation 17]
t+F(y,L,du,p)
=x-F(y,L,du,p)+F(y,L,du,p)
= Generate the ticket judging information M to show that x, next the ticket judging information generation section 203 hold the right ticket from the additional information L of a ticket, and the information on an internal state (S212). The certification information generation section 206 generates the following values as certification information (S213, S214).
[0101]
[Equation 18] T= (C||M) and Cx mod p -- in addition, the certification information T is calculable with the following formulas besides the above.
[0102]
[Equation 19]
T= (C||M) and CtCF (y, L, du, p) mod p and the authentication information generation section 204 generate random-number r' to coincidence, and are [0103].
[Equation 20] Chi=gr' mod p is sent to verification equipment as 2nd authentication information (S215, S216, S205). The information included in the ticket judging information M is the same as that of examples 1-3.
[0104] The certification information T and the 2nd authentication information chi are sent to verification equipment 100 by the communications department 208.
[0105] The verification equipment 100 which received T and chi performs ticket judging processing (S206 of drawing 20).
[0106] The flow chart of ticket judging processing is shown in drawing 22 . It is [0107] from the ticket certification information that the certification information verification section 103 of verification equipment 100 was sent in drawing 22 .
[Equation 21] T/yr mod p= (C||M) and Cx/yr mod The value of p is calculated and it checks whether parts other than M connected among the bit string are in agreement with the authentication information C (S221). When in agreement, the ticket judging section 101 judges further whether it is what the internal state related with the ticket and the ticket may verify with this verification equipment 100 from the contents of the ticket judging information M (S222, S223). When this ticket may be verified as a result of a judgment, the certification information generation section 103 creates the information mu which directs modification of the internal state of certification equipment 200, and connects it with chi (S224, S225). And the following values are generated as 2nd authentication information to this value using the confidential information xi showing the privilege of verification equipment (S226).
[0108]
[Equation 22]

$$\rho = (\chi \,||\, \mu) \cdot \chi^{E} \mod p$$

rho is sent to certification equipment 200 by the communications department 106. On the other hand, when ticket certification information is not a right thing, or in being what a ticket should not verify, it ends a protocol (S227).
[0109] Next, the certification equipment 200 which received rho performs internal-state modification processing (S208 of drawing 20).
[0110] The flow chart of internal-state modification processing is shown in drawing 23 . It is [0111] from a response indication to which the certification information verification section 205 of certification

equipment 200 was sent in drawing 23 .
[Equation 23]
$\rho / \eta^{r'} \mod p = (\chi \| \mu) \cdot \chi^{r} / \eta^{r'} \mod p$

A ** value is calculated and it checks whether parts other than mu connected among the bit string are in agreement with the 2nd authentication information chi (S231). When it is able to be checked that it is a right thing, according to the information the internal-state control section 207 instructs modification of the internal state of mu to be, the internal state of certification equipment 200 changes and the result is made into M' (S232-S234). On the other hand, as a result of a check, when it becomes clear that it is not right, a protocol is ended to a case (S137).
[0112] after the certification information generation section 206 connects the value of M' with the bit string of the authentication information C -- the following values -- certification information -- ** -- it generates by carrying out (S235, S236).
[0113]
[Equation 24] R= (C||M') and Cx mod p -- the certification information R generated in this way is sent to verification equipment 100 by the communications department 208 (S209).
[0114] The verification equipment 100 which received R performs certification information verification processing S210 (drawing 20).
[0115] The flow chart of certification information verification processing is shown in drawing 24 . It is
[0116] from the ticket certification information that the certification information verification section 104 was sent in drawing 24 .
[Equation 25] R/yr mod The value of p= (C||M') and Cx/yrr mod p is calculated and, as a result, the bit string of the high order except M' checks that it is in agreement with the authentication information C which verification equipment 100 generated first (S241). The defined service is offered, when it checks whether the contents of information M' which expresses the modification result of an internal state further are in agreement with the information mu to which internal-state modification sent as 2nd certification information rho is permitted when it is able to check (S242, S243, S244) and a check is completed (S245). When one of checks goes wrong, a protocol is completed and offer of service is not performed (S246).

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is a flow chart explaining processing of a related technique.
[Drawing 2] It is the block diagram showing the configuration of examples 1, 2, and 4 as a whole.
[Drawing 3] It is a flow chart explaining the whole processing of an example 1.
[Drawing 4] It is a flow chart explaining ticket certification information generation processing of the certification equipment of an example 1.
[Drawing 5] It is a flow chart explaining ticket judging processing of the verification equipment of an example 1.
[Drawing 6] It is a flow chart explaining internal-state modification processing of the certification equipment of an example 1.
[Drawing 7] It is a flow chart explaining certification information verification processing of the verification equipment of an example 1.
[Drawing 8] It is drawing showing the internal state in early stages of the token of an example 2.
[Drawing 9] It is drawing showing the item of ticket additional information.
[Drawing 10] It is drawing showing the ticket judging information M sent to a ticket gate machine from a token at the time of entrance.
[Drawing 11] It is drawing showing the item mu sent to a token from a ticket gate machine at the time of entrance.
[Drawing 12] It is drawing showing the internal state of the token after entrance.
[Drawing 13] It is drawing showing the ticket judging information M sent to a ticket gate machine from a token at the time of participation.
[Drawing 14] It is drawing showing the information mu sent to a token from a ticket gate machine at the time of participation.
[Drawing 15] It is drawing showing the internal state of the token after participation.
[Drawing 16] It is the block diagram showing the configuration of an example 3 as a whole.
[Drawing 17] It is a flow chart explaining ticket certification information generation processing of the certification equipment of an example 3.
[Drawing 18] It is a flow chart explaining ticket judging processing of the verification equipment of an example 3.
[Drawing 19] It is a flow chart explaining internal-state modification processing of the certification equipment of an example 3.
[Drawing 20] It is the flow chart which shows processing of an example 4 as a whole.
[Drawing 21] It is a flow chart explaining ticket certification information generation processing of the certification equipment of an example 4.
[Drawing 22] It is a flow chart explaining ticket judging processing of the verification equipment of an example 4.
[Drawing 23] It is a flow chart explaining an internal-state update process of the certification equipment of an example 4.

[Drawing 24] It is a flow chart explaining certification information verification processing of the verification equipment of an example 4.
[Description of Notations]
100 Verification Equipment
101 Ticket Judging Section
102 Authentication Information Generation Section
103 Certification Information Generation Section
104 Certification Information Verification Section
200 Certification Equipment
201 Certification Equipment Proper Information Attaching Part
202 Ticket Attaching Part
202a Counter
203 Ticket Judging Information Generation Section
204 Authentication Information Generation Section
205 Certification Information Verification Section
206 Certification Information Generation Section
207 Internal-State Control Section
300 Ticket Assignment Equipment

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－225143

(43)公開日　平成11年(1999)８月17日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ
Ｇ０６Ｆ　17/60		Ｇ０６Ｋ　17/00	Ｔ
Ｇ０６Ｋ　17/00			Ｓ
		Ｇ０７Ｂ　1/00	Ａ
Ｇ０７Ｂ　1/00			Ｂ

審査請求　未請求　請求項の数41　ＯＬ　（全 29 頁）　最終頁に続く

(21)出願番号　特願平10－27074

(22)出願日　平成10年(1998)２月９日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　木子　健一郎
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　中垣　寿平
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

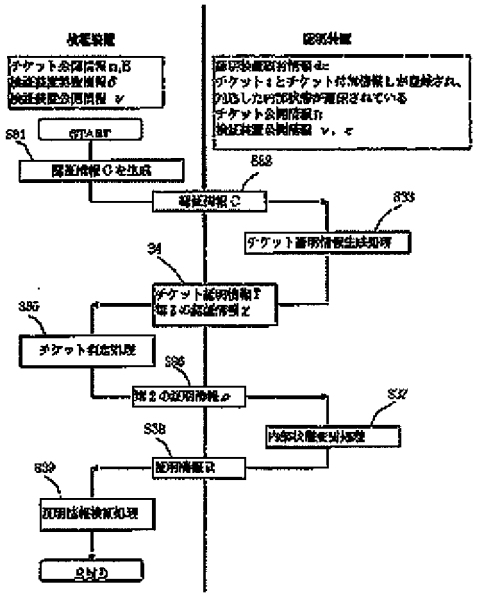
(72)発明者　京嶋　仁樹
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内

(74)代理人　弁理士　澤田　俊夫

最終頁に続く

(54)【発明の名称】　電子チケットシステム

(57)【要約】
【課題】　誤って、または不正に提示されたチケットにより証明装置の内部状態が変更されないようにする。
【解決手段】　検証装置１００の認証情報生成部１０２が、認証情報Ｃを生成し証明装置２００に送る（Ｓ３１、Ｓ３２）。証明装置２００のチケット判定情報生成部２０３は、正しいチケットを保持していることを示すためのチケット判定情報Ｍを、チケット利用情報および内部状態記憶領域の情報から生成する。証明情報生成部２０６は、認証情報Ｃのビット列の下位にチケット判定情報Ｍを連結し、チケット証明情報Ｔを生成する（Ｓ３３）。チケット証明情報Ｔは、通信部２０８により検証装置１００に送られる（Ｓ３４）。Ｔを受け取った検証装置１００はチケット判定処理を行い、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないものの場合には、プロトコルを終了する（Ｓ３５）。



実施例１の処理全体のフローチャート

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開
特開平11－
(43)公開日　平成11年(

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ
Ｇ０６Ｆ　17/60		Ｇ０６Ｋ　17/00	Ｔ
Ｇ０６Ｋ　17/00			Ｓ
		Ｇ０７Ｂ　1/00	Ａ
Ｇ０７Ｂ　1/00			Ｂ

審査請求　未請求　請求項の数41　ＯＬ　（全 29 頁）

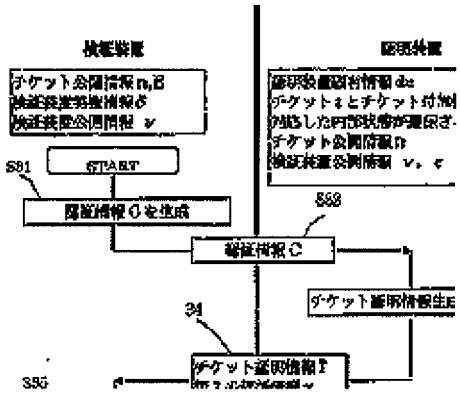
(21)出願番号　特願平10－27074

(22)出願日　平成10年(1998)２月９日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22
(72)発明者　木子　健一郎
神奈川県足柄上郡中井町境43(
テクなかい　富士ゼロックス
(72)発明者　中垣　寿平
神奈川県足柄上郡中井町境43(
テクなかい　富士ゼロックス
(72)発明者　京嶋　仁樹
神奈川県足柄上郡中井町境43(
テクなかい　富士ゼロックス
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　電子チケットシステム

(57)【要約】
【課題】　誤って、または不正に提示されたチケットにより証明装置の内部状態が変更されないようにする。
【解決手段】　検証装置１００の認証情報生成部１０２が、認証情報Ｃを生成し証明装置２００に送る（Ｓ３１，Ｓ３２）。証明装置２００のチケット判定情報生成部２０３は、正しいチケットを保持していることを示すためのチケット判定情報Ｍを、チケット利用情報および内部状態記憶領域の情報から生成する。証明情報生成部２０６は、認証情報Ｃのビット列の下位にチケット判定



1

【特許請求の範囲】

【請求項１】　証明装置と検証装置とを有し、上記証明装置が正当なチケットを所有していることを検証する電子チケットシステムであって、

上記証明装置は、

上記証明装置の固有情報を保持する証明装置固有情報保持手段と、

上記チケットを保持するチケット保持手段と、

上記チケットの権利内容または上記チケットの使用状態を表すチケット判定情報を生成するチケット判定情報生成部と、

少なくとも上記証明装置固有情報と上記チケットとからチケット秘密情報を生成し、上記チケット秘密情報を用いて証明情報を生成する証明情報生成手段とを有し、

上記検証装置は、

上記証明装置が提示する上記チケット判定情報に基づいて、検証処理を実行して良いかを判定するチケット判定手段と、

上記証明装置がチケット秘密情報を生成できたか否かを、上記証明情報に基づいて、検証する証明情報検証手段とを有することを特徴とする電子チケットシステム。

【請求項２】　請求項１に記載の電子チケットシステムであって、

上記検証装置は、対話証明で用いられる認証情報を生成する認証情報生成手段を有し、

上記証明装置の証明情報生成手段は、上記検証装置が生成した認証情報を用いて上記証明情報を生成する電子チケットシステム。

【請求項３】　請求項２に記載の電子チケットシステムであって、上記証明装置と上記検証装置とは通信手段を有し、上記証明装置は証明しようとするチケットのチケット判定情報を、上記検証装置に伝送する電子チケットシステム。

【請求項４】　請求項２ないし３に記載の電子チケットシステムであって、

上記電子チケットシステムは、上記検証装置と上記証明装置とに加えて、チケット発行装置を有し、

上記チケット発行装置は、

発行するチケットの秘密の特徴情報である上記チケット秘密情報と対応するチケット公開情報を保持するチケット特徴情報保持手段と、

利用者が保持する上記証明装置の固有情報を保持するチケット発行用証明装置固有情報保持手段と、

上記チケット特徴情報保持手段に保持している上記チケット秘密情報と、上記チケット発行用証明装置固有情報保持手段に保持している上記証明装置固有情報とを用いて、デジタル情報であるチケットを作成するチケット発行手段をを有する電子チケットシステム。

【請求項５】　請求項２ないし４の電子チケットシステムであって、上記証明装置の証明情報生成手段は、少なくとも上記検証装置から送られた認証情報と、上記チケットと、上記チケット判定情報と、上記証明装置固有情報とより所定の方法で、上記証明情報の１つとして、上記チケット判定手段の判定に用いるチケット証明情報を計算する電子チケットシステム。

2

【請求項６】　請求項５に記載の電子チケットシステムであって、上記証明装置はチケットの利用条件を定めたチケット利用情報を、チケットと対応させて上記チケット保持部に保持する電子チケットシステム。

【請求項７】　請求項５に記載の電子チケットシステムであって、上記証明装置は、上記チケット判定情報を作成する際に、少なくとも上記チケット利用情報を用いる電子チケットシステム。

【請求項８】　請求項６に記載の電子チケットシステムであって、上記証明装置は、可変な内部状態を保持する内部状態記憶領域と、上記内部状態の値を制御する内部状態制御手段とを備える電子チケットシステム。

【請求項９】　請求項８に記載の電子チケットシステムであって、上記証明装置のチケット判定情報生成手段は、上記チケット判定情報を作成する際に、少なくとも上記証明装置の内部状態記憶領域の情報を用いる電子チケットシステム。

【請求項１０】　請求項８ないし９の電子チケットシステムであって、上記証明装置の内部状態記憶領域が保持する可変な内部状態のうちの、少なくとも一部は外部から書き換え不能である電子チケットシステム。

【請求項１１】　請求項８ないし１０の電子チケットシステムであって、上記証明装置の証明情報生成手段は、少なくとも、上記チケットと、上記チケット利用情報と、上記証明装置固有情報とを用いて上記証明情報を計算する電子チケットシステム。

【請求項１２】　請求項８ないし１１の電子チケットシステムであって、上記証明装置は、上記検証手段から送られた上記認証情報を保持する認証情報保持手段を有し、上記証明情報生成手段は、上記チケット判定情報生成手段により生成されたチケット判定情報を用いて、上記認証情報保持手段に保持されている認証情報を変更して上記証明情報の生成に利用する電子チケットシステム。

【請求項１３】　請求項１２の電子チケットシステムであって、上記チケット判定情報生成手段が生成したチケット判定情報をＭとし、上記認証情報をＣとすると、上記証明装置の証明情報生成手段は、上記認証情報保持手段に保持されている認証情報Ｃを、ＣにＭを接合したものに更新する電子チケットシステム。

【請求項１４】　請求項１２ないし１３の電子チケットシステムであって、上記証明装置の証明情報生成手段は、上記証明情報の１つとしてチケット証明情報を生成することが可能であり、上記チケット証明情報は、上記チケットと、上記チケット利用情報と、上記証明装置固

有情報とより所定の方法でチケット秘密情報を計算し、上記認証情報に対して、チケット秘密情報を用いた計算を施すことによって生成される電子チケットシステム。

【請求項１５】　請求項１４の電子チケットシステムであって、ｐ、ｑが素数であり、ｎ＝ｐ・ｑであり．ＤＥ≡１　ｍｏｄ　（ｐ－１）（ｑ－１）の関係が満たされるとき、上記チケット秘密情報がＤであり、チケット公開情報が（ｎ．Ｅ）であり．上記チケット利用情報がＬであり、上記証明装置固有情報が秘密の値ｄｕであり、ｆ（ｄｕ，Ｌ．ｎ）を一方向性関数として、チケットがｔ＝Ｄ－ｆ（ｄｕ，Ｌ，ｎ）で与えられているとき、上記証明装置の証明情報生成手段は、上記認証情報Ｃ（上記証明情報生成手段が変更した認証情報）に対して、Ｃの法ｎでのｔによる冪乗と．Ｃの法ｎでの一方向性関数値ｆ（ｄｕ，Ｌ．ｎ）による冪乗との法ｎでの積$C^{t}C^{f(du,L,n)}$　ｍｏｄ　ｎとしてチケット証明情報を計算する電子チケットシステム。

【請求項１６】　請求項１４の電子チケットシステムであって、ｐ、ｑが素数であり、ｎ＝ｐ・ｑであり．ＤＥ≡１　ｍｏｄ　（ｐ－１）（ｑ－１）の関係が満たされるとき、上記チケット秘密情報がＤであり、チケット公開情報が（ｎ．Ｅ）であり．上記チケット利用情報がＬであり、上記証明装置固有情報が秘密の値ｄｕであり、ｆ（ｄｕ，Ｌ．ｎ）を一方向性関数として、上記チケットがｔ＝Ｄ－ｆ（ｄｕ，Ｌ．ｎ）で与えられているとき．上記証明装置は、あらかじめｔ＋ｆ（ｄｕ．Ｌ．ｎ）＝Ｄを計算し、その値を用いて．上記認証情報Ｃ（上記証明情報生成手段が変更した認証情報）に対して．Ｔ＝C^{D}　ｍｏｄ　ｎとしてチケット証明情報Ｔを計算する電子チケットシステム。

【請求項１７】　請求項１４の電子チケットシステムであって、ｇが離散対数問題が困難な群の原始根であり、ｐが素数であり．整数ｘに対してｙ＝g^{x}ｍｏｄ　ｐが成り立つとき．上記チケット秘密情報がｘであり．チケット公開情報が（ｙ，ｐ、ｇ）であり．上記チケット利用情報がＬであり、上記証明装置固有情報が秘密の値ｄｕであり、ｆ（ｄｕ，Ｌ．ｙ）を一方向性関数として、上記チケットがｔ＝ｘ－ｆ（ｄｕ，Ｌ．ｙ）で与えられているとき、上記証明装置は、上記認証情報Ｃ（上記証明情報生成手段が変更した認証情報）に対して．上記チケット判定情報ＴをＣの法ｐでのｔによる冪乗と．Ｃの法ｐでの一方向性関数値ｆ（ｄｕ，Ｌ．ｙ）を指数とする冪乗との法ｐでの積$C^{t}C^{f(du,t,y)}$　ｍｏｄｎとして上記証明情報を計算する電子チケットシステム。

【請求項１８】　請求項１４の電子チケットシステムであって、ｇが離散対数問題が困難な群の原始根であり、ｐが素数であり．整数ｘに対してｙ＝g^{x}ｍｏｄ　ｐが成り立つとき．上記チケット秘密情報がｘであり．チケット公開情報が（ｙ，ｐ、ｇ）であり．上記チケット利用情報がＬであり、上記証明装置固有情報が秘密の値ｄ

ｕであり、ｆ（ｄｕ，Ｌ．ｙ）を一方向性関数として、上記チケットがｔ＝ｘ－ｆ（ｄｕ，Ｌ．ｙ）で与えられているとき、上記証明装置は、あらかじめｔ＋ｆ（ｄｕ，Ｌ，ｙ）＝ｘを計算し．上記認証情報Ｃに対して（上記証明情報生成手段が変更した認証情報）チケット判定情報Ｔを計算する際に．C^{x}　ｍｏｄ　ｐの値を用いる電子チケットシステム。

【請求項１９】　請求項１４ないし１８の電子チケットシステムであって、上記検証装置の証明情報検証手段は．上記認証情報生成手段が作成した認証情報と．上記証明装置から送られたチケット証明情報と、上記チケット公開情報とより、上記チケット証明情報の正当性を検証し．上記チケット証明情報が正しい場合は、上記チケット証明情報に埋め込まれたチケット判定情報を導出する電子チケットシステム。

【請求項２０】　請求項１９の電子チケットシステムであって、上記認証情報がＣであり、上記チケット証明情報がＴであり．上記チケット公開情報（ｎ、Ｅ）であり．あるビット列Ｍがある場合に、上記検証装置の証明情報検証手段は．上記チケット証明情報Ｔを法ｎでＥでべき乗したものをＣとＭとを接合したビット列と比較し．T^{e}　ｍｏｄ　ｎ＝Ｃ｜｜Ｍ（記号｜｜はビット列の接合）となっていれば．上記チケット証明情報は正しいと判定し、上記チケット証明情報が正しい場合はＭを上記チケット判定情報として導出する電子チケットシステム。

【請求項２１】　請求項１９の電子チケットシステムであって、上記認証情報がＣであり、上記チケット証明情報がＴであり．上記チケット公開情報が（ｐ，ｇ、ｙ）である場合に．上記検証装置の証明情報検証手段は、自身が発生させた乱数をｒとするとき．あるビット列Ｍがあって、Ｔ／y^{r}　ｍｏｄ　ｐ＝（Ｃ｜｜Ｍ）（記号｜｜はビット列の接合）となっていれば、上記チケット証明情報は正しいと判定し．上記チケット証明情報が正しい場合はＭをチケット判定情報として導出する電子チケットシステム。

【請求項２２】　請求項８ないし２１の電子チケットシステムであって．

上記証明装置は．上記検証装置を認証するための第２の認証情報を生成する、第２の認証情報生成手段と．上記検証装置が生成する第２の証明情報を検証するための、第２の証明情報検証手段とを有し、

上記第２の証明情報検証手段は、上記第２の認証情報と．上記第２の証明情報と．チケット公開情報とより上記第２の証明情報が正しいかどうかを検証し、

上記第２の証明情報が正しい場合、上記内部状態制御手段は．上記証明装置の内部状態を変更する電子チケットシステム。

【請求項２３】　請求項２２の電子チケットシステムであって、上記検証装置の証明情報検証手段は、上記チケ

ット判定手段による判定の結果をもとにして、上記第２の証明情報を生成するか否かを決定する電子チケットシステム。

【請求項２４】 請求項２２の電子チケットシステムであって、

上記証明装置は、チケットのカウンタとして機能する内部状態をチケットと関連づけ、外部から書き換え不能な形で、内部状態記憶領域に保持し、

上記検証装置の証明情報検証手段は、上記証明装置から送られたチケット判定情報に含まれる内部状態のカウンタの値が、所定の値であるときには、対応するチケットが無効であるものと判断する電子チケットシステム。

【請求項２５】 請求項２２ないし２４の電子チケットシステムであって、p'、q'が素数であり、$\nu = p' \cdot q'$であり、$\delta\varepsilon \equiv 1 \mod (p'-1)(q'-1)$の関係が満たされるときに、上記証明装置の第２の証明情報検証手段は、上記第２の認証情報χと上記第２の証明情報ρが

【数１】

$$\chi = \rho^{\varepsilon} \mod \nu$$

を満たす場合に上記第２の証明情報が正しいと判定する電子チケットシステム。

【請求項２６】 請求項２２ないし２４の電子チケットシステムであって、gが離散対数問題が困難な群の原始＊根であり、pが素数であり、整数ξに対して

【数２】

$$\eta = g^{\xi} \mod p$$

が成り立つときに、証明装置の第２の認証情報生成手段は、乱数r'と上記第２の認証情報$\chi = g^{r'}$を生成し、上記第２の証明情報検証手段は上記第２の証明情報ρについて、$\rho / \eta^{r'} \mod p = \chi$が満たされた場合に上記第２の証明情報が正しいと判定する電子チケットシステム。

【請求項２７】 請求項２２の電子チケットシステムであって、上記証明装置の第２の証明情報検証手段は、上記第２の証明情報が正しい場合は、上記第２の証明情報に埋め込まれた情報を導出する電子チケットシステム。

【請求項２８】 請求項２７の電子チケットシステムであって、上記証明装置の第２の証明情報検証手段は、上記第２の証明情報から導出された情報を、上記内部情報の変更を許可するための情報として利用する電子チケットシステム。

【請求項２９】 請求項２７ないし２８の電子チケットシステムであって、チケット公開情報はνおよびεを含んでおり、上記証明装置の第２の証明情報検証手段は、上記第２の認証情報χと上記第２の証明情報ρとが、あるビット列μに対して、

【数３】

$$\chi \| \mu = \rho^{\varepsilon} \mod \nu$$ (記号$\|$はビット列の接合)

を満たすときに、上記第２の証明情報が正しいと判定し、μを上記第２の証明情報に埋め込まれた情報として導出する電子チケットシステム。

【請求項３０】 請求項２７の電子チケットシステムであって、上記証明装置の内部状態制御手段は、上記第２の証明情報から導出された情報にもとづいて上記内部状態記憶領域に保持された内部状態を変更する電子チケットシステム。

【請求項３１】 請求項３０の電子チケットシステムであって、上記証明装置の上記第２の証明情報検証手段は、上記検証装置より送られた内部状態変更を許可する情報と、内部状態とに基づいて、上記証明情報を正しく生成するか否かを判定する電子チケットシステム。

【請求項３２】 請求項２２ないし３１の電子チケットシステムであって、上記検証装置は、上記検証装置の特権を表す秘密情報である、検証装置特権情報を保持する検証装置特権情報保持部と、上記第２の証明情報を生成する第２の証明情報生成部を有し、

上記第２の証明情報生成部は、上記第２の認証情報と上記検証装置特権情報とより第２の証明情報を生成する電子チケットシステム。

【請求項３３】 請求項３２の電子チケットシステムであって、上記検証装置特権情報をδとし、対応する公開情報を(ν, ε)とするとき、上記検証装置の第２の証明情報生成部は、上記第２の認証情報χより上記第２の証明情報ρを

【数４】

$$\rho = \chi^{\delta} \mod \nu$$

として生成する電子チケットシステム。

【請求項３４】 請求項３２の電子チケットシステムであって、上記検証装置特権情報をξ、対応する公開情報を(p, g, η)とし、

【数５】

$$\eta = g^{\xi} \mod p$$

の関係が満たされるとき、上記検証装置の第２の証明情報生成部は上記第２の認証情報χに対して、

【数６】

$$\chi^{\xi} \mod p$$

の値を用いて上記第２の証明情報ρを生成する電子チケットシステム。

【請求項３５】 請求項３２ないし３４の電子チケットシステムであって、上記検証装置は上記第２の認証情報を保持する、第２の認証情報保持部を有し、上記検証装置の第２の証明情報生成部は、上記検証装置特権情報を用いた計算を施す際に、証明装置の内部状態の変更を許可する情報と、上記第２の認証情報より上記第２の証明情報を計算する電子チケットシステム。

【請求項３６】 請求項３２ないし３４の電子チケットシステムであって、上記検証装置の第２の証明情報生成部は、上記検証装置特権情報を用いた計算を施す前に、

上記証明装置の内部状態の変更を許可する情報を用いて、上記第２の認証情報保持部に保持された上記第２の認証情報を更新する電子チケットシステム。

【請求項３７】　請求項３６の電子チケットシステムであって、上記検証装置の第２の証明情報生成部は、上記証明装置の内部状態の変更を許可する情報をμとし、上記第２の認証情報をχとすると、上記第２の認証情報保持部に保持された第２の認証情報をχにμを接合したものに更新する電子チケットシステム。

【請求項３８】　請求項１ないし３７に記載の電子チケットシステムであって、少なくとも、上記証明装置が、内部のデータ及び処理手続きを外部から観測することを困難ならしめる防御手段中に保持されている電子チケットシステム。

【請求項３９】　請求項ないし３７に記載の電子チケットシステムであって、少なくとも、上記証明装置が、ＩＣカードなどの携帯可能な小型演算装置として構成されている電子チケットシステム。

【請求項４０】　証明装置と検証装置とを有し、上記証明装置が正当なチケットを所有していることを検証する電子チケットシステムであって、

上記証明装置は、

上記証明装置の固有情報を保持する証明装置固有情報保持手段と、

上記チケットを保持するチケット保持手段と、

上記チケットの権利内容または上記チケットの使用状態を表すチケット判定情報を生成するチケット判定情報生成部と、

少なくとも上記証明装置固有情報と上記チケットとから証明情報を生成する証明情報生成手段とを有し、

上記検証装置は、

上記証明装置が提示する上記チケット判定情報に基づいて、検証処理を実行して良いかを判定するチケット判定手段と、

上記証明装置が上記証明装置固有情報と上記チケットから上記証明情報を生成できたか否かを検証する証明情報検証手段とを有することを特徴とする電子チケットシステム。

【請求項４１】　検証装置と電子チケットを保持する認証装置との間で相互認証を行ないながら検証装置側で所

【発明の属する技術分野】本発明は、チケットを電子的に作成し利用する技術に関する。

【０００２】

【背景の技術】〔従来の技術〕近年、乗車指定券、予約券、回数券、定期券、プリペイドカード、などの一般的なチケットとして発行する試みが行われている。

【０００３】このような電子チケットは、利用者に与えた権利を特定でき、正しいチケットであることを検証できるという機能を持つ。電子情報は容易であり、通信回線を通して送信できる特性を持つが、完全なコピーを簡単に作れるのでチケットの実現には、偽造と複製による不正利用の防止が不可欠である。電子署名により偽造の防止は可能だが、複製の防止は困難であり、複製による不正利用を防ぐことが、電子チケットの実現にあたっての課題となっていた。

【０００４】この問題に対する、解決策としてチケットの利用時に正当な利用者か確認する第１の従来技術、発行者以外の者にチケットを複写されない第２の従来技術、検証時の通信を公開鍵暗号を用いた第２の従来技術を修正した第３の従来技術などの方法が提案されてきた。

【０００５】第１の従来技術は、チケットの利用者が、正当な利用者かどうかを確認するものである。利用者は、チケットを利用する時に、チケットに、自分が利用者特定情報に適合する正当な利用者であることを示す。利用者特定情報に適合した利用者にのみ利用する権利の行使が認められる。確認のために利用者特定情報（利用者特定情報）と、与えた権利とを対応づけたものがチケットとして発行され、利用者が記憶する。発行者以外の者が勝手にチケットを偽造できないようにするためには、発行者がチケットに電子署名を施す。署名のないチケットは、偽造されたものとして扱う。利用者特定情報には、身元、顔写真などの生体情報、パスワードなどの知識の所有などが利用される。

【０００６】しかしながら、この方法では、利用者特定情報に応じて、いくつかの問題がある。

【０００７】例えば、利用者特定情報に生体情報を利用する方法では、発行時と検証時に利用

【００６９】第２の従来技術は、例えば特開平８－１４７５００号公報に示されるようなものであり、発行者以外の者にチケットを複写する機会を与えない方法である。この方法では、利用者が保持管理しているチケットを複写できないようにする機構と、発行時や検証時の通信からチケットが漏洩しない機構の両方を必要とする。

【００７０】しかしながら、この方法では

（１）発行者以外の者はチケットを複写できないので、チケットの正当性を第三者に証明することが困難になる。（２）チケットの発行時と検証時の通信の内容も機密に行うので、チケットの発行時と検証時にプライバシーなどの利用者の権利が侵害されていないことを証明できない、といった問題点が生ずる。

【００７１】第３の従来技術は、例えば特公平６－５２５１８号公報に示されるようなものであり、検証時の通信を公開できるように、第２の従来技術を修正した方法である。この方法では、第２の従来技術と同様に、チケットを秘密情報として利用者の所持する装置（証明装置）に複写できないように記録するが、検証の方法が異なっている。まず、検証を行う検証装置は、証明装置に乱数などの繰り返し利用されない値（チャレンジ）を送る。証明装置は、チケットである秘密情報を利用した演算をチャレンジに対して施して、得られた値（レスポンス）を検証装置に送り返す。検証装置は、秘密情報とチャレンジを利用してレスポンスが演算されたことを確認することで、利用者の正当性を認証する。レスポンスから逆に秘密情報を求めることを計算量的に困難とすることで、チャレンジとレスポンスを秘密通信とする必要がなくなる。

【００７２】この方法は、認証のために利用されるものであり、正当なチケットを保持しているか否か以外に情報を伝達しない。このため、有効期限などを示すことができず、単純なチケットしか表現できない。また、チケットを証明装置に送信する方法が、第２の従来技術と同様に機密通信で行う必要があり、不当に利用者の情報を開示して利用者の権利を侵害していないことを証明できないという問題があった。

【００７３】このように、従来の技術はいずれも、チケットに必要な不正利用を防止する機能を実現するために、第三者に対するチケットの内容証明の機能や利用者の匿名性を犠牲にしている点に、問題があった。

【００７４】〔関連技術〕これらの問題を解決する関連技術として、特願平９－１８８０６４号（平成９年７月１４日、未公開）に示す方法が提案されている。

【００７５】この関連技術の一般的な認証プロトコルを図１に示す。このプロトコルは、双方向の認証を行うプロトコルであり、双方が認証情報（発生した乱数）に対する署名を確認することによって、お互いの正当性を認証する。相互の認証情報（乱数）の一部にメッセージ（ｍ，μ）を含ませることにより、情報の安全な伝達を可能にしている。

【００７６】図１を参照して関連技術のプロトコルについて説明する。図１において、はじめに、検証装置が乱数に基づいて認証情報Ｃを生成し（Ｓ１１）、この認証情報Ｃを証明装置に対して送る（Ｓ１２）。他方、証明装置は乱数に基づいて別の認証情報χを生成し、認証情報χを検証装置に送る（Ｓ１３、Ｓ１４）。証明装置にはチケットに対応して、外部からは操作不能な内部状態があり、検証装置からの応答情報によってのみ書き換えが可能となっている。検証装置はχの一部に、内部状態の変更を許可する情報（μ）を含ませた応答情報を作成し、検証装置が署名して証明装置に送る（Ｓ１５，Ｓ１６）。証明装置は応答情報ρの署名を確認することにより、送信者が正当な検証装置であることを確認し、それをもって内部状態変更の情報μの正しさを確認する（Ｓ１７）。ρが正しい場合にのみ、証明装置の内部状態がμの内容にしたがって変更される（Ｓ１８）。証明装置は、正当に作成されたチケットｔと証明装置固有情報ａｕから、Ｄを復元することが可能であり（Ｓ１９）、最後に証明情報ＲにＤによる署名を施して、検証装置に送り（Ｓ２０、Ｓ２１）、検証装置はその署名を確認することにより、定められたサービスを提供する（Ｓ２２，Ｓ２３）。

【００７７】この方法によれば、チケットの検証情報は公開であるため第３者にもチケットの検証が可能であり、利用者はチケットの検証時に利用者を特定する情報を提示する必要が無いことから、匿名性も守られている。

【００７８】また、検証装置と証明装置がそれぞれの秘密情報と公開情報を持ち合い、相互の認証をすることにより、証明装置・検証装置の偽造の問題を解決している。さらに、この証明に用いる認証情報の一部に、伝達したい情報を埋め込むことにより、検証装置－証明装置相互の情報伝達をも可能にしており、チケットの内容を証明することができる。

【００７９】このように、この関連技術の方法を使うと、電子チケットの基本的な機能をすべて満たした安全な電子チケットを実現することができ、上記の問題をすべて解決することが可能である。

【００８０】ところで、先の関連技術では、検証装置がチケットを特定する情報を証明装置に送ることにより、検証装置が検証しようとするチケットが証明装置の中で一意に定まることを前提としている。しかし、実際には、その検証装置で検証可能なチケットが証明装置内に複数存在することも考えられる。たとえば、鉄道の乗車券のようなものを考えた場合、その駅から有効な回数券や定期券など複数のチケットが証明装置の中に存在することがありうる。そのような場合、証明装置では、どのチケットを利用者が利用しようとしているのか判断することができない。そこで、こういった場合には、利用者

があらかじめ利用するチケットを選択する必要が生ずる。

【００２１】そして、このような場面において、先の関連技術を適用すると、チケットに対応する内部状態の変更を許可する応答情報が、選択・提示されたチケットの内容を確認することなしに作成され、送られてしまうという問題が生ずる。

【００２２】これは、例えば、利用者が誤ったチケットを選択してしまった場合に、意図しないチケットの内部状態が変更されてしまうことを意味している。

【００２３】また、鉄道の切符に適用する場合を考えると、内部状態として、入場の記録を残しておき、出場時に入場の記録を確認することにより、キセルのような不正行為を防止することが考えられる。

【００２４】ここで、入場の情報として、単に入場したという事実のみを、チケットに対応する内部状態に残すような場合を考える。このような場合、内部状態の変更許可情報、具体的には入場情報を、提示されたチケットの内容を確認すること無く証明装置に送ってしまうと、本来その駅では入場できないチケットに対しても、入場したという事実を残すことが可能になる。実際には正当でないチケットでの入場はできないが、入場を拒否された段階で、内部状態が書き換えられたチケットを保持している証明装置を手に入れることができるとすると、実際に入場した駅よりも目的駅に近い駅からのチケットに対する入場記録を偽造すれば、出場時に偽造した入場記録を持つチケットを提示することで、キセル行為が可能になってしまう。

【００２５】このように、利用者が、証明しようとするチケットを自ら選択するような場合には、検証装置は、内部状態を変更する許可情報を作成する前に、提示されたチケットがその検証装置で正当に検証可能であることを確認する必要がある。

【００２６】しかし、先の関連技術においては、このような確認が成されないため、利用者が誤って意図しないチケットに対応する内部状態を書き換えてしまったり、内部状態を書き換えることによる不正が可能であったりするという問題点があった。

【００２７】

【発明が解決しようとする課題】本発明では、上記の問題を解決するために、検証装置が検証可能なチケットのみを検証し、検証することが正しくないチケットに対しては、内部状態の変更を許可する情報を生成しないような電子チケットシステムを実現することを目的とする。

【００２８】

【課題を解決するための手段】上記の課題を解決するため、本発明に係わる電子チケットシステムは、チケット検証装置と証明装置からなり、チケット検証装置は、検証するチケットが検証装置で検証可能かどうかを、証明装置が提示するチケット判定情報に基づいて判定するチケット判定手段と、証明装置がチケット秘密情報を算出できたか否かを検証する対話検証手段を有し、証明装置は、証明装置固有情報保持手段と、チケット保持手段と、少なくとも証明装置固有情報とチケットからチケット秘密情報に関する知識の証明を行える対話証明手段とを有している。

【００２９】この構成においては、検証装置が、チケット判定情報に基づいて、証明装置内のチケットの適合性をチェックでき、正しいチケットが提示されたときのみ証明装置の内部状態を変更するようにできる。

【００３０】

【発明の実施の態様】以下、本発明を詳細に説明する。

【００３１】〔実施例１〕図２に本発明の実施例１の電子チケットシステムの構成図を示す。図２において、本実施例に示す電子チケットシステムは、検証装置（検証器ともいう）１００と証明装置（証明器ともいう）２００とチケット指定装置３００とからなる。

【００３２】検証装置１００は、検証するチケットの正当性を判定するチケット判定部１０１と、認証情報生成部１０２と、証明情報生成部１０３と、証明情報検証部１０４と、検証装置特権情報保持部１０５と、通信部１０６とを含んで構成される。

【００３３】一方、証明装置２００は、証明装置固有情報保持部２０１と、チケット保持部２０２と、チケット判定情報生成部２０３と、認証情報生成部２０４と、証明情報検証部２０５と、証明情報生成部２０６と、内部状態制御部２０７と、通信部２０８とを含んで構成される。なお検証装置１００の証明情報生成部１０３、認証装置２００の証明情報生成部２０６は、それぞれ認証装置２００、検証装置１００から送られてくる認証情報を保持する記憶部を具備している。

【００３４】また、チケット保持部２０２にはチケットと、各チケットに対応するチケット利用情報とが保存される。また、チケット保持部２０２には各チケットに対応する内部状態記憶領域が確保される。

【００３５】ここでは、証明装置２００は、内部のデータや処理手続きを外部から観測することが困難なＩＣカードのような媒体により構成される。

【００３６】また、この実施例では以下のように、チケットｔが発行される。

【００３７】

【表１】

チケット：$t = D - F(n, L, du)$

Ｄ：チケット秘密鍵

ｄｕ：証明装置固有の秘密情報

ｎ：チケット任数

Ｆ：非衝突性一方向関数

Ｌ：チケット利用情報

ただし、

$ED \equiv 1 \bmod n$

ここでＥ：チケット公開鍵
である。チケット秘密情報がＤであり，チケット公開情報は，Ｅ，ｎ，Ｌである。Ｆは一般のハッシュ関数によって実現可能である。また，チケット利用情報Ｌには，そのチケットを利用する条件，例えば有効期限や，サービスを受けられる場所などの情報が入る。

【００３８】本発明の認証プロトコルの概略を図３に示す。はじめに利用者は，これから利用するチケットをチケット指定装置３００により証明装置２００に指定した上で，検証装置１００と証明装置２００との間で認証プロトコルが開始される。

【００３９】図３において，認証プロトコルでは，まず検証装置１００の認証情報生成部１０２が，認証情報として乱数Ｃを生成し証明装置２００に送る（Ｓ３１，Ｓ３２）。

【００４０】認証情報を受け取った証明装置２００は，チケット証明情報生成処理を実行する（Ｓ３３）。

【００４１】チケット証明情報生成処理（Ｓ３３）のフローチャートを図４に示す。図４において，まず証明装置２００の証明情報生成部２０６は，署名に用いる秘密鍵Ｄを，チケットｔとチケット利用情報Ｌおよび証明装置固有情報保持部２０１に保存されている証明装置固有情報ｄｕから，以下の計算により算出する（Ｓ４１）。

【００４２】
【数７】
$$t+F(n, L, du) = D-F(n, L, du)+F(n, L, du) = D$$
次に，チケット判定情報生成部２０３は，正しいチケットを保持していることを示すためのチケット判定情報Ｍを，チケット保持部２０２のチケット利用情報および内部状態記憶領域の情報から生成する（Ｓ４２）。証明情報生成部２０６は，認証情報Ｃのビット列の下位にチケット判定情報Ｍを連結し（Ｓ４３），チケット証明情報Ｔを，

【００４３】
【数８】$T=(C||M)^{e} \bmod n$
の計算により生成する（Ｓ４４，なお記号｜｜はビット列に連結することを示す）。なお上記の計算以外にも，

【００４４】
【数９】$T=(C||M)^{t}(C||M)^{F(n,L,du)} \bmod n$
により，証明情報Ｔを計算しても良い。

【００４５】また，認証情報生成部２０４は，乱数χを生成し第２の認証情報とする（Ｓ４４）。

【００４６】チケット証明情報Ｔと第２の認証情報χは，通信部２０８により検証装置１００に送られる（Ｓ３４）。署名をするのは，チケット証明情報が正しいものであり，証明装置・チケット判定情報が偽造されていないことを保証するためである。

【００４７】Ｔとχを受け取った検証装置１００はチケット判定処理（図３のＳ３５）を行う。

【００４８】チケット判定処理（図３のＳ３５）のフローチャートを図５に示す。図５において，検証装置１００の証明情報検証部１０４は，送られたチケット証明情報Ｔと証明情報検証部が保持しているチケット公開情報Ｅから，

【００４９】
【数１０】$T^{t} \bmod n$
の値を計算し，そのビット列のうち，連結された上位ビットの部分が，認証情報Ｃと一致するかどうかを確認する（Ｓ５１）。一致した場合には，さらにチケット判定情報Ｍを抽出する（Ｓ５２）。次に，チケット判定部１０１は，Ｍの内容をもとにチケット及びチケットに関連付けられた内部状態がこの検証装置で検証して良いものかどうかを判定する（Ｓ５３）。判定の結果，このチケットを検証して良い場合には，証明情報生成部１０３は，証明装置２００の内部状態の変更を指示する情報μを作成して，χの下位に連結する（Ｓ５４，Ｓ５５）。さらに，この値に対して，検証装置の特権を表す秘密情報δを用いて署名をした値ρを作成する（Ｓ５６）。作成されたρは，通信部１０６により証明装置２００へと送られる（Ｓ３６）。

【００５０】一方，チケット証明情報が正しいものでない場合や，チケットが検証すべきでないものの場合には，プロトコルを終了する（Ｓ５７）。

【００５１】次にρを受け取った証明装置は内部状態変更処理（図３のＳ３７）を行う。

【００５２】内部状態変更処理（図３のＳ３７）のフローチャートを図６に示す。図６において，証明装置２００の証明情報検証部２０５は，送られた第２の証明情報ρに対して，自身が保持している検証装置１００の特権を確認する公開情報εを用いて

【００５３】
【数１１】
$$\rho^{\varepsilon} \bmod \nu$$
を計算し，そのビット列のうち，上位の部分が，第２の認証情報χと一致するかどうかを確認する（Ｓ６１）。確認の結果，正しくないことが判明した場合には場合には，プロトコルを終了する（Ｓ６２）。正しいものであることが確認できた場合には，連結されたμを抽出する（Ｓ６３）。内部状態制御部２０７は，μの内容に応じて証明装置２００の内部状態を変更し，その結果をＭ'とする（Ｓ６４，Ｓ６５），証明情報生成部２０６はＭ'の値を認証情報Ｃのビット列に連結した上で，

【００５４】
【数１２】$R=(C||M')^{e} \bmod n$
の計算により，証明情報Ｒを生成する（Ｓ６６，Ｓ６７），Ｒは通信部２０８により検証装置１００に送られる（Ｓ３８），

【００５５】Ｒを受け取った検証装置１００は，証明情報検証処理（図３のＳ３９）を行う。

【００５６】証明情報検証処理（図３のＳ３９）のフローチャートを図７に示す。図７において、検証装置１００の証明情報検証部１０４は保持しているチケット公開情報Ｅを用いて，

【００５７】

【数１３】$R^{t} \mod n$

の値を計算し，その結果追結されたM'を除いた上位のビット列が，最初に検証装置１００が生成した認証情報Ｃと一致することを確認する（Ｓ７１）。確認できた場合は，さらに内部状態の変更結果を表す情報M'の内容が，第２の証明情報ρとして送った，内部状態変更を許可する情報μと一致するかどうかを確認し（Ｓ７２，Ｓ７３，Ｓ７４），確認ができた場合には，定められたサービスを提供する（Ｓ７５）。いずれかの確認に失敗した場合には，プロトコルが終了し，サービスの提供は行われない（Ｓ７１，Ｓ７４，Ｓ７６）。

【００５８】［実施例２］本発明の実施例２は，実施例１を鉄道の切符の改札券として実現した場合である。ここでは特に、乗車券の入場時のプロトコルを説明する。

【００５９】本発明の実施例の構成やチケットの生成方法は実施例１と同様であるが，検証装置１００は具体的には自動改札機であり，証明装置２００はチケットを保持することができる，ＩＣカードのようなトークンである。そして，入場，出場ともに自動改札による検証が行われ，内部状態には入場や出場に対応した記憶領域が確保されるものとする。

【００６０】以下では，横浜～成田空港１９９７年７月１８日の乗車券の例で説明する。なお，通宜，図３の対応するステップ等を指摘する。

【００６１】チケットのチケット利用情報Ｌは，図９のようになる。チケットは証明装置２００に登録されており，対応した内部状態記憶領域が確保されている。入場前の内部状態を図８に示す。ここで，これから使用するチケットは，チケットＩＤが００００５に示すものである。

【００６２】まず，入場時の認証について説明する。はじめに検証装置１００は認証情報Ｃとともに，入場であることをあらわす情報を証明装置２００に送る（Ｓ３２）。

【００６３】証明装置２００は，チケット判定情報Ｍを生成する。Ｍの内容を図１０に示す。チケット判定情報Ｍには，図に示すように，チケット利用情報に含まれる内容と，使用状態を示すための，内部状態の入場・出場記録の内容が含まれている。証明情報生成部２０６は，ＭをＣに連結し，チケット秘密鍵Ｄによる署名を施して，チケット証明情報Ｔとして，生成した第２の認証情報χとともに検証装置１００に送る（Ｓ３４）。

【００６４】検証装置１００は，チケット証明情報を検証し，さらにチケット判定情報Ｍの内容を確認する。ここでは，入場駅が横浜駅で，有効期限内であり，未使用のチケットであることから，ここでの認証をしてよいチケットであると判定される（Ｓ３５）。

【００６５】そこで，証明装置２００の内部状態を変更するための情報μが作成される。μの内容を図１１に示す。μには，入場駅名と時間が記録される。証明情報生成部１０３は，こうして生成したμを第２の認証情報χに連結し，検証装置１００の特権情報δによる署名を施した値ρを生成して，証明装置２００へ送る（Ｓ３６）。

【００６６】証明装置２００の証明情報検証部２０５は，送られたρの値が，認証情報χと一致するかどうかを確認する。正しいものであることが確認できた場合には，内部状態制御部２０７がμの内容に応じて，証明装置２００の内部状態を変更する（Ｓ３７）。変更後の内部状態の様子を図１２に示す。入場の駅と時間が記録されたことがわかる。次に，内部状態制御部２０７はこの内部状態の変更，すなわち入場記録の内容をM'とする。実施例１と同様に、証明情報生成部２０６は，M'の値を認証情報のビット列に連結して，チケット秘密情報による署名を施した値Ｒを生成して，証明情報Ｒとして検証装置１００に送る（Ｓ３８）。

【００６７】検証装置１００は証明情報Ｒの値を検証し，その値が認証情報Ｃと一致した場合には，さらに内部状態を変更した結果M'を確認する。M'がμで指定したものと対応していれば，正しく内部状態が変更されたものと判断し，改札機のゲートを開ける。

【００６８】次に、出場時の認証を説明する。出場時の認証は、入場時とほぼ同様であるが，相互に伝えられるメッセージの内容が異なる。

【００６９】はじめに検証装置１００は認証情報Ｃとともに，出場であることをあらわす情報を証明装置に送る（Ｓ３２）。

【００７０】証明装置２００のチケット判定情報生成部２０３はチケット判定情報Ｍを生成する。出場時のＭの内容を図１３に示す。証明情報生成部２０６は，ＭをＣに連結し，チケット秘密鍵Ｄによる署名を施し，チケット証明情報Ｔとする。そして，証明情報Ｔと，認証情報生成部生成した第２の認証情報χが検証装置に送られる（Ｓ３４）。

【００７１】検証装置１００の証明情報検証部１０４は，チケット証明情報を検証する。チケットの検証結果が正しい場合には，チケット判定部１０１が，チケット判定情報Ｍの内容を確認する。ここでは，入場駅が横浜駅で有効な入場記録であり，出場の有効期間内であることから，ここでの出場の認証が可能なチケットであると判定される（Ｓ３５）。

【００７２】次に，証明情報生成部１０３は証明装置２００の内部状態を変更するための情報μを作成する。μ

の内容を図14に示す。μには、出場駅名と出場時間が記録される。証明情報生成部103は、さらに、生成されたμをχに連結し、検証装置の特権情報δによる署名を施した値ρを生成する。ρは証明装置200へと送られる（S36）。

【0073】証明装置200の証明情報検証部205は、送られたρの値が、認証情報χと一致するかどうかを確認する。正しいことが確認できた場合には、内部状態制御部207がμの内容に応じて、証明装置200の内部状態を変更し、この変更結果、すなわち出場記録をM'とする。変更後の内部状態の様子を図15に示す。出場駅と時間が記録される。証明情報生成部206は、出場記録M'を認証情報Cのビット列に連結して、チケット秘密情報による署名を施した証明情報Rを生成し、検証装置100に送る（S38）。

【0074】検証装置200の証明情報検証部104はRの値を検証し、その値が認証情報Cと一致した場合には、さらに内部状態を変更した結果M'を確認する。M'がμの値で指定したものと対応していれば、正しく内部状態が変更されたものと判断し、出場を許可して、改札機のゲートを開ける（S39）。

【0075】〔実施例3〕実施例3では、回数券のような形態を実現する方法を示す。

【0076】基本的には本実施例の構成やチケットの生成方法、全体の処理の流れは実施例1と同様である。本実施例の全体の構成を図16に示す。本実施例の特徴として、内部状態の中に、回数券の残り度数を示すカウンタ202aが設置されている点が異なる。図16においては、図2と対応する箇所に対応する符号を付した。

【0077】利用者は回数券を購入すると、はじめに証明装置200に登録する。登録時に回数券に対応する内部状態記憶領域が確保され、そのなかのカウンタ202aに、残りの使用回数が書き込まれる。

【0078】回数券の利用時には利用者は、証明装置200に対してこれから利用するチケットとして、チケット指定装置300により、回数券を指定した上で、検証装置100と証明装置200との間で認証プロトコルが開始される。

【0079】認証プロトコルでは、検証装置100が、認証情報として乱数Cを生成し証明装置200に送り、証明装置200が、チケット秘密鍵を計算するところまでは、実施例1と同様である。

【0080】本実施例のチケット証明情報生成処理（図3のS33に対応）のフローチャートを図17に示す。図17において、証明装置200のチケット判定情報生成部203は、この回数券のチケットに対応した内部状態の残り回数を抽出し、チケット利用情報とともに、チケット判定情報Mに記録する（S81～S84）。そして、実施例1と同様に、証明情報生成部206がチケット証明情報Tを生成し（S85）、認証情報生成部204が第2の認証情報χを生成する（S86）。Tとχは通信部208により検証装置100に送られる（S34）。

【0081】Tとχを受け取った検証装置100はチケット判定処理（図3のS35に対応す）を行う。

【0082】チケット判定処理のフローチャートを図18に示す。図18において、検証装置100の証明情報検証部104は、受け取ったチケット証明情報を検証する（S91）。チケット証明情報が正しい場合には、チケット証明情報から、チケット判定情報Mを抽出する（S92）。チケット判定情報Mには回数券の残り回数が記録されている。チケット判定部101はその値が1以上であれば、この回数券はまだ使用可能であると判断する（S93）。さらに、チケット利用情報Lの内容も、この検証装置100で検証可能であるとチケット判定部101が判断した場合には、証明情報生成部103は証明装置200の内部状態の変更を指示する情報μを作成する（S94、S95）。μの内容として、回数券の使用回数を1減らすことを指示する内容が含まれる。そして、実施例1と同様の方法で、μを使用して第2の証明情報ρを作成し（S96、S97）、証明装置200へと送る（S36）。

【0083】検証やチケット判定に失敗したときにはエラー処理を行なう（S98）。

【0084】ρを受け取った証明装置200は内部状態変更処理（図3のS37に対応）を行う。

【0085】内部状態変更処理のフローチャートを図19に示す。図19において、証明装置200の証明情報検証部205は送られた第2の証明情報ρを検証する（S101）。正しいものであることが確認できた場合には、内部状態制御部がμの内容に応じて、回数券の残り使用回数を1減らし、その結果をM'とする（S102～S104）。あとは、実施例1と同様の方法で、証明装置200は証明情報Rを生成して、検証装置100に送る（S105、S106）。ステップS101で検証に失敗したときにはエラー処理が行なわれる（S107）。

【0086】以降の検証装置100の動作は、実施例1と同様であり、Rの値を検証して、サービスの提供を行う。

【0087】〔実施例4〕本発明の実施例4では、全体の構成は実施例1と同様であるが、チケット公開情報・チケット秘密情報やチケットの認証方法が異なる。

【0088】本実施例では、pが素数であり、Gが離散対数問題が困難な有限群であり、gが有限群Gの位数pの元であり、

【0089】

【数14】$y = g^{x} \bmod p$

が満たされるとき、（p，G，g，y）がチケット公開情報であり、xをチケット秘密情報とする。（p，G，

g）はシステム全体で共通とすることもできる。

【0090】このとき、チケットはチケット特徴情報xと証明装置固有情報duとチケット利用情報Lと、群を規定する情報pより、

【0091】

【数15】$t = x - F(du, L, y, p)$

として、計算される。ここで、Fは非衝突性の一方向関数であり、一般のハッシュ関数によって実現可能である。Lは実施例1と同様のチケット利用情報である。

【0092】また、検証装置の特権をあらわすものとして、上記（p，G，g）は共通として、

【0093】

【数16】$$\eta = g^{\xi} \mod p$$

を満たすようなηを公開情報、ξを秘密情報とする。

【0094】実際にはGを乗法群として構成したり、有限体上の楕円曲線として構成することができる。

【0095】本発明の認証プロトコルの概略を図20に示す。

＊【0096】はじめに利用者は、これから利用するチケットを証明装置に対して指定した上で、検証装置と証明装置の間で認証プロトコルが開始される。

【0097】図20において、この認証プロトコルでは、まず検証装置100の認証情報生成部102が、乱数rを生成し、$C = g^r$を計算して、これを認証情報として証明装置に送る（S201、S202、S203）。

【0098】認証情報Cを受け取った証明装置200は、チケット証明情報生成処理を実行する（S204）。

【0099】チケット証明情報生成処理のフローチャートを図21に示す。図21において、まず証明装置200の証明情報生成部206は、署名に用いる秘密鍵xを、チケットtとチケット利用情報L、チケット公開情報のp、および証明装置固有情報duから、以下の計算により算出する（S211）。

【0100】

【数17】

$$\begin{aligned} & t + F(y, L, du, p) \\ &= x - F(y, L, du, p) + F(y, L, du, p) \\ &= x \end{aligned}$$

次に、チケット判定情報生成部203は、正しいチケットを保持していることを示すためのチケット判定情報Mを、チケットの付加情報Lや内部状態の情報から生成する（S212）。証明情報生成部206は、証明情報として、以下の値を生成する（S213，S214）。

【0101】

【数18】$T = (C \| M) \cdot C^{x} \mod p$

なお証明情報Tは上記以外にも、以下の式によっても計算できる。

【0102】

【数19】$T = (C \| M) \cdot C^{t} C^{F(y, L, du, v)} \mod p$

また、認証情報生成部204は同時に乱数r'を生成して、

【0103】

【数20】$\chi = g^{r'} \mod p$

を第2の認証情報として検証装置に送る（S215、S216、S205）。チケット判定情報Mに入る情報は実施例1～3と同様である。

【0104】証明情報Tと第2の認証情報χは、通信部208により検証装置100に送られる。

【0105】Tとχを受け取った検証装置100はチケット判定処理（図20のS206）を行う。

【0106】チケット判定処理のフローチャートを図22に示す。図22において、検証装置100の証明情報検証部103は、送られたチケット証明情報から、

【0107】

【数21】$T / y^{r'} \mod p = (C \| M) \cdot C^{x} /$ $y^{r'} \mod p$

の値を計算し、そのビット列のうち、連結されたM以外の部分が、認証情報Cと一致するかどうかを確認する（S221）。一致した場合には、チケット判定部101はさらにチケット判定情報Mの内容から、チケット及びチケットに関連付けられた内部状態がこの検証装置100で検証して良いものかどうかを判定する（S222，S223）。判定の結果、このチケットを検証して良い場合には、証明情報生成部103は証明装置200の内部状態の変更を指示する情報μを作成して、χに連結する（S224、S225）。そして、この値に対して、検証装置の特権を表す秘密情報ξを用いて以下の値を第2の認証情報として、生成する（S226）。

【0108】

【数22】$$\rho = (\chi \| \mu) \cdot \chi^{\xi} \mod p$$

ρは通信部106により証明装置200へと送られる。一方、チケット証明情報が正しいものでない場合や、チケットが検証すべきでないものの場合には、プロトコルを終了する（S227）。

【0109】次にρを受け取った証明装置200は内部状態変更処理（図20のS208）を行う。

【0110】内部状態変更処理のフローチャートを図23に示す。図23において、証明装置200の証明情報検証部205は、送られた応答情報から、

【0111】

【数23】

21　　22

$$\rho/\eta^{r'} \mod p = (\chi \| \mu) \cdot \chi^{r}/\eta^{r'} \mod p$$

の値を計算し，そのビット列のうち，追補されたμ以外の部分が，第２の認証情報χと一致するかどうかを確認する（Ｓ２３１）。正しいものであることが確認できた場合には、内部状態制御部２０７が，μの内部状態の変更を指示する情報に応じて，証明装置２００の内部状態が変更し、その結果をM'とする（Ｓ２３２～Ｓ２３４）。一方、確認の結果，正しくないことが判明した場合には場合には，プロトコルを終了する（Ｓ１３７）。

【０１１２】証明情報生成部２０６は，M'の値を認証情報Cのビット列に連結した上で，以下の値を証明情報をとして生成する（Ｓ２３５、Ｓ２３６）。

【０１１３】

【数２４】$R = (C \| M') \cdot C^{x} \mod p$

こうして生成された証明情報Rが通信部２０８により検証装置１００に送られる（Ｓ２０９）。

【０１１４】Rを受け取った検証装置１００は，証明情報検証処理Ｓ２１０（図２０）を行う。

【０１１５】証明情報検証処理のフローチャートを図２４に示す。図２４において，証明情報検証部１０４は、送られたチケット証明情報から、

【０１１６】

【数２５】$R/y^{r'} \mod p = (C \| M') \cdot C^{x}/y^{r}r \mod p$

の値を計算し，その結果M'を除いた上位のビット列が，最初に検証装置１００が生成した認証情報Cと一致することを確認する（Ｓ２４１）。確認できた場合は、さらに内部状態の変更結果を表す情報M'の内容が、第２の証明情報ρとして送った、内部状態変更を許可する情報μと一致するかどうかを確認し（Ｓ２４２，Ｓ２４３，Ｓ２４４），確認ができた場合には、定められたサービスを提供する（Ｓ２４５）。いずれかの確認に失敗した場合には，プロトコルが終了し，サービスの提供は行われない（Ｓ２４６）。

【０１１７】

【発明の効果】以上で説明したように，本発明によれば，検証装置が検証可能なチケットのみを検証し，検証することが正しくないチケットに対しては、内部状態の変更を許可する情報を生成しないような電子チケットシステムを実現することができ、利用者の意図しない内部状態の変更や，内部状態の変更による不正行為を防止することができる。

【図面の簡単な説明】

【図１】　関連技術の処理を説明するフローチャートである。

【図２】　実施例１，２，４の構成を全体として示すブロック図である。

【図３】　実施例１の処理全体を説明するフローチャートである。

【図４】　実施例１の証明装置のチケット証明情報生成処理を説明するフローチャートである。

【図５】　実施例１の検証装置のチケット判定処理を説明するフローチャートである。

【図６】　実施例１の証明装置の内部状態変更処理を説明するフローチャートである。

【図７】　実施例１の検証装置の証明情報検証処理を説明するフローチャートである。

【図８】　実施例２のトークンの初期の内部状態を示す図である。

【図９】　チケット付加情報の項目を示す図である。

【図１０】　入場時にトークンから改札機に送られるチケット判定情報Mを示す図である。

【図１１】　入場時に改札機からトークンに送られる項目μを示す図である。

【図１２】　入場後のトークンの内部状態を示す図である。

【図１３】　出場時にトークンから改札機に送られるチケット判定情報Mを示す図である。

【図１４】　出場時に改札機からトークンに送られる情報μを示す図である。

【図１５】　出場後のトークンの内部状態を示す図である。

【図１６】　実施例３の構成を全体として示すブロック図である。

【図１７】　実施例３の証明装置のチケット証明情報生成処理を説明するフローチャートである。

【図１８】　実施例３の検証装置のチケット判定処理を説明するフローチャートである。

【図１９】　実施例３の証明装置の内部状態変更処理を説明するフローチャートである。

【図２０】　実施例４の処理を全体として示すフローチャートである。

【図２１】　実施例４の証明装置のチケット証明情報生成処理を説明するフローチャートである。

【図２２】　実施例４の検証装置のチケット判定処理を説明するフローチャートである。

【図２３】　実施例４の証明装置の内部状態更新処理を説明するフローチャートである。

【図２４】　実施例４の検証装置の証明情報検証処理を説明するフローチャートである。

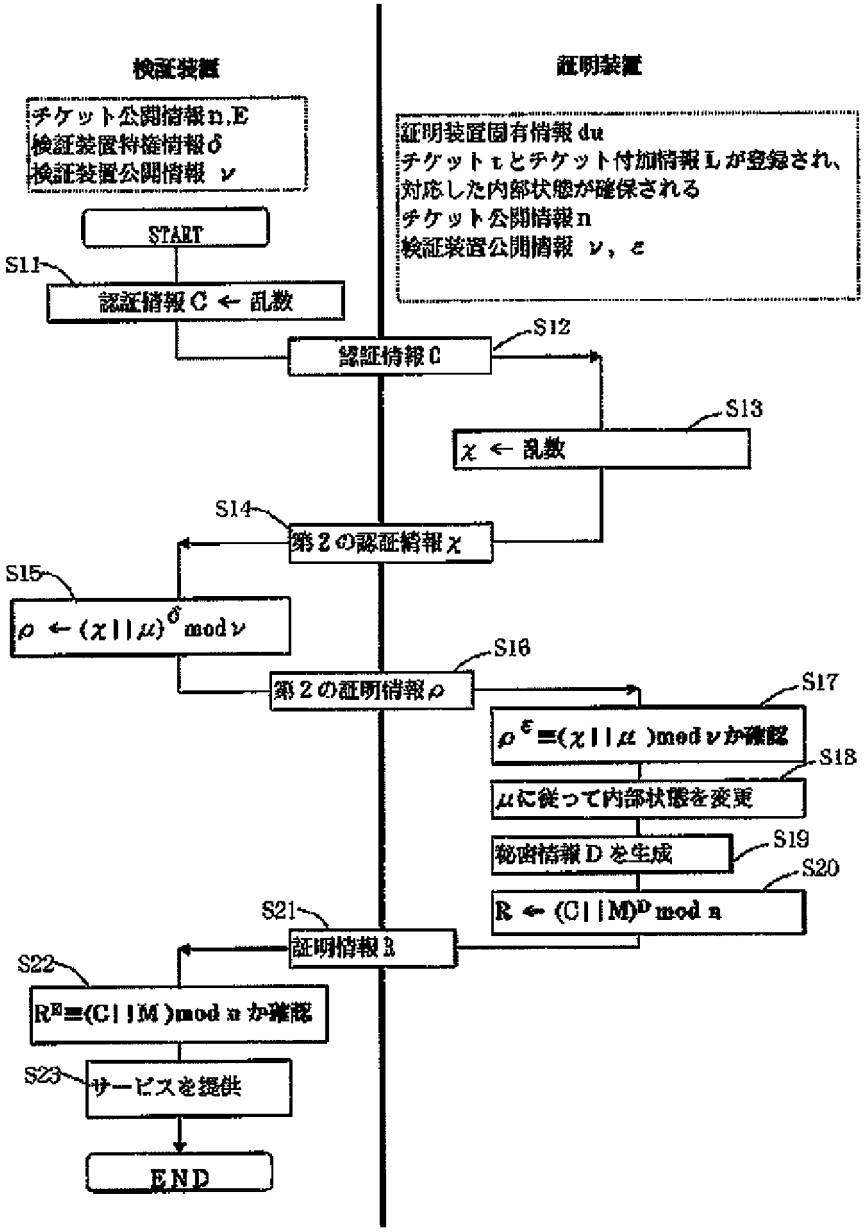
【符号の説明】

１００　検証装置
１０１　チケット判定部
１０２　認証情報生成部
１０３　証明情報生成部
１０４　証明情報検証部
２００　証明装置
２０１　証明装置固有情報保持部
２０２　チケット保持部

23 24

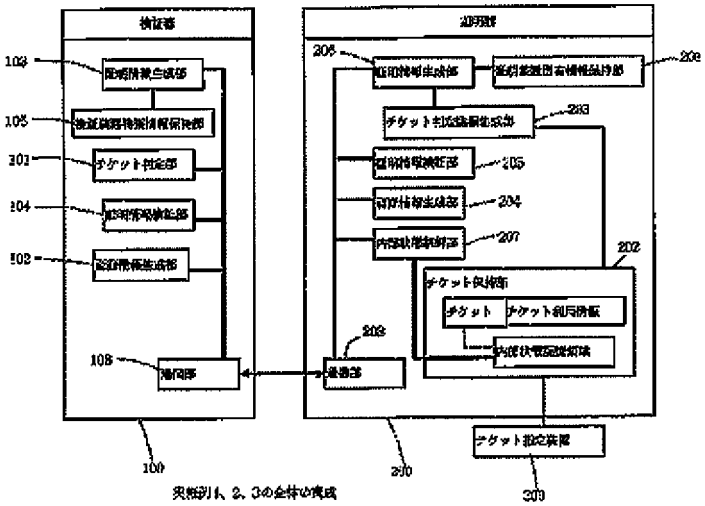
２０２ａ　カウンタ
２０３　チケット判定情報生成部
２０４　認証情報生成部
２０５　証明情報検証部
＊２０６　証明情報生成部
２０７　内部状態制御部
３００　チケット指定装置
＊

【図１】



関連技術の処理のフローチャート

【図２】



【図８】

トークンの初期の内部状態

チケットID	基準情報	課金形態	変更履歴	入場日時	出場日時	検札結果
00001	97/8/31	現金	なし	なし	なし	なし
00003	97/8/31	クレジットカード	なし	97/8/31,9:05 横浜	97/8/31,5:32 平塚	なし
00099	97/8/10	現金	なし	なし	なし	なし

【図１０】

入場時にトークンから券売機に送られるチケット特定情報_M

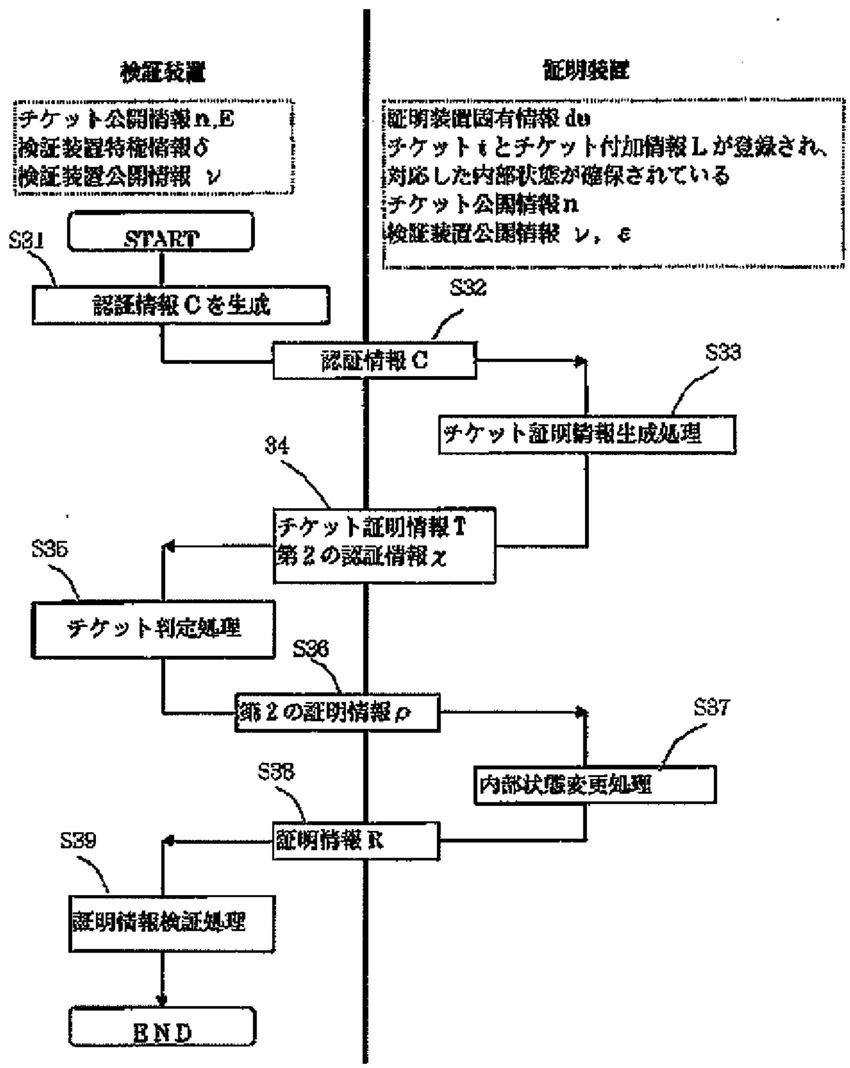
出発駅	目的駅	使用開始日	有効期間	経路	入場記録	出場記録	検札記録
横浜	成田空港	97/7/18	1日	東京	なし	なし	なし

【図９】

チケット利用情報の項目

発行NO	発券場所	課金形態	出発駅	目的駅	発行日時	使用開始日	有効期間	経路
00123	平塚	現金	横浜	成田空港	97/7/10	97/7/18	1日	東京

【図3】



実施例１の処理全体のフローチャート

【図11】

入場時に改札機からトークンに送られる情報μ（横浜駅で入場）

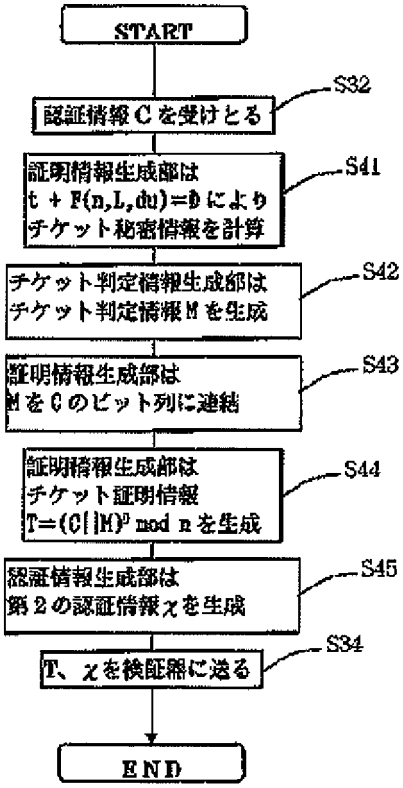
入場駅	入場時刻
横浜	97/7/19,6:30

【図12】

入場後のトークンの内部状態

チケットID	発券情報	料金形態	変更記録	入場記録	出場記録	検札記録
00001	97/6/31	現金	なし	なし	なし	なし
00008	97/6/31	クレジットカード	なし	97/6/31, 9:05 横浜	97/6/31, 9:30 平塚	なし
00015	97/7/19	現金	なし	97/7/19, 6:25 横浜	なし	なし

【図４】



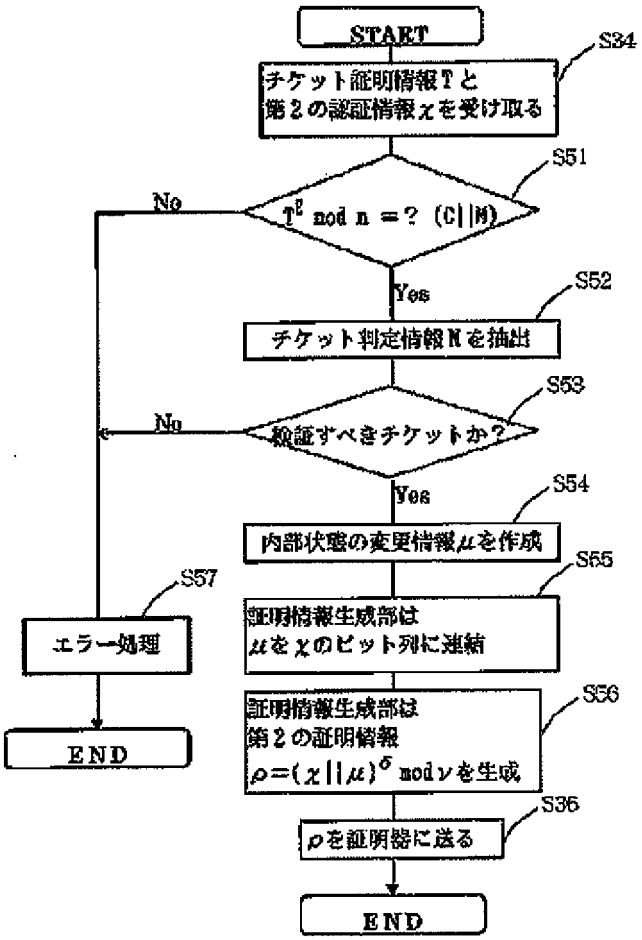
実施例１の証明装置のチケット証明情報生成処理のフローチャート

【図１３】

出場時にトークンから改札機に送られるチケット判定情報 M

出発駅	目的駅	使用開始日	有効期間	経路	入場記録	出場記録	検札記録
横浜	成田空港	97/7/18	1日	東京	97/7/18,6:20 横浜	なし	なし

【図５】



実施例１の検証装置のチケット判定処理のフローチャート

【図１４】

乗降駅	出場時間
成田空港	97/7/18,8:53

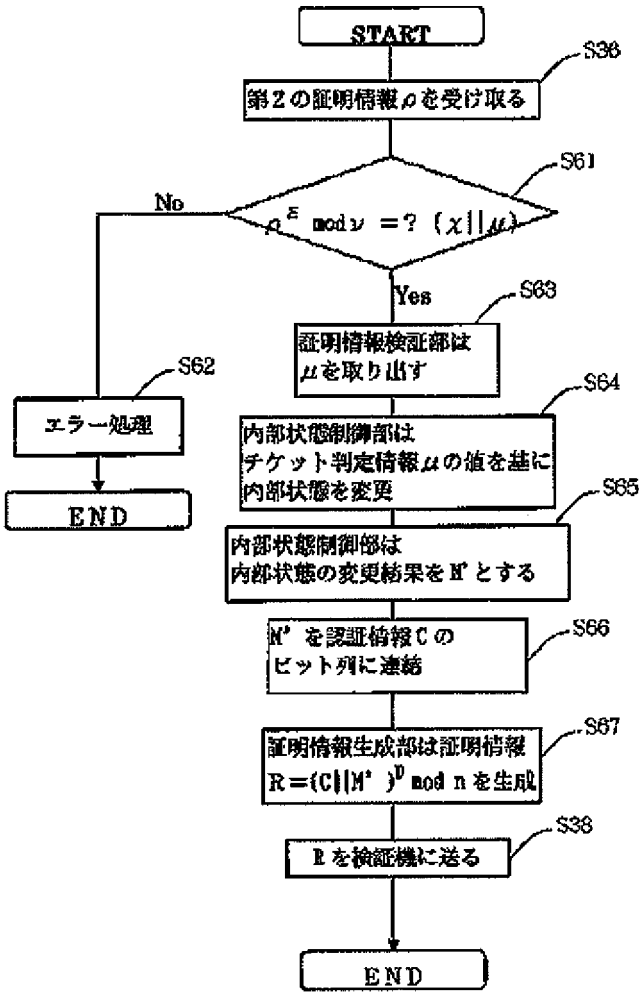
出場時に改札機からトークンに送られる情報（成田空港で出場）

【図１５】

出場後のトークンの内部状態

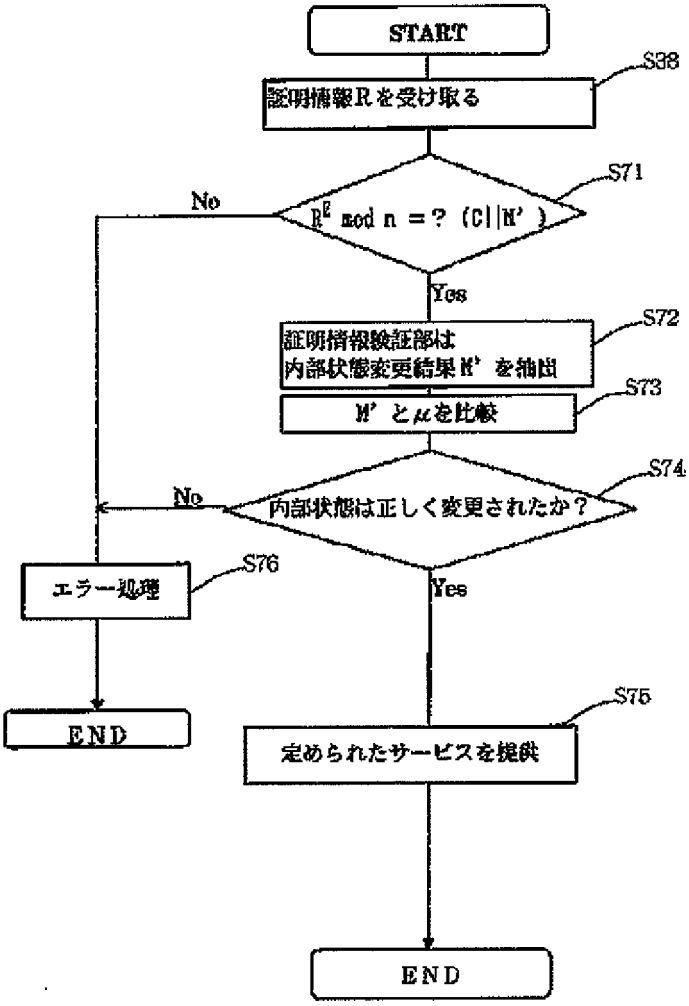
チケットID	残高情報	精算手段	定期記録	入場記録	出場記録	抽札記録
00001	97/6/31	現金	なし	なし	なし	なし
00008	97/6/31	クレジットカード	なし	97/6/31,9:15 横浜	97/6/30,9:20 平塚	なし
00005	97/7/10	現金	なし	97/7/18,6:29 横浜	97/7/18,8:53 成田空港	なし

【図6】



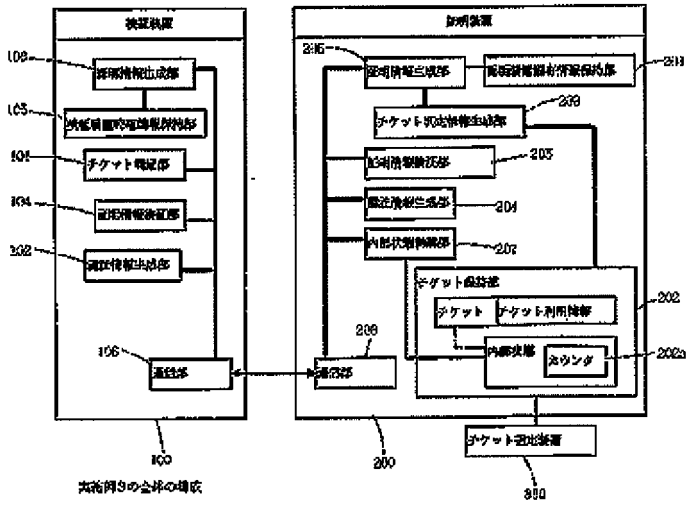
実施例1の証明装置の内部状態変更処理のフローチャート

【図7】

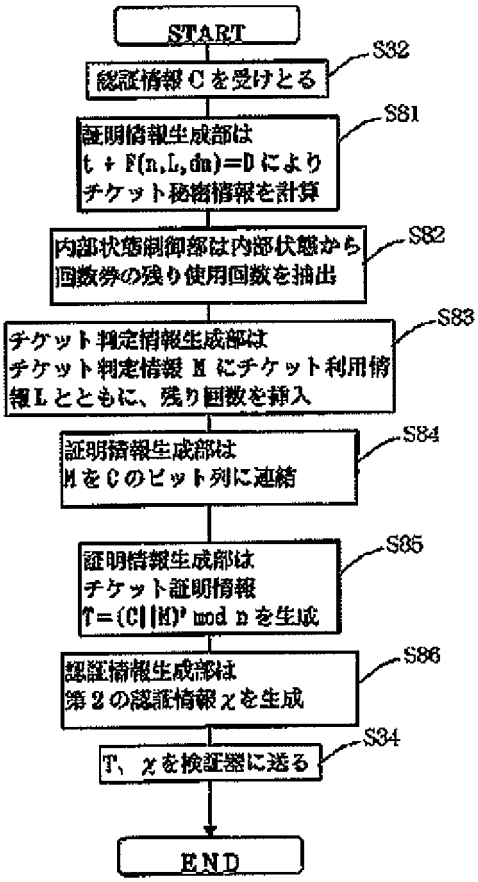


実施例1の検証装置の証明情報検証処理のフローチャート

【図１６】

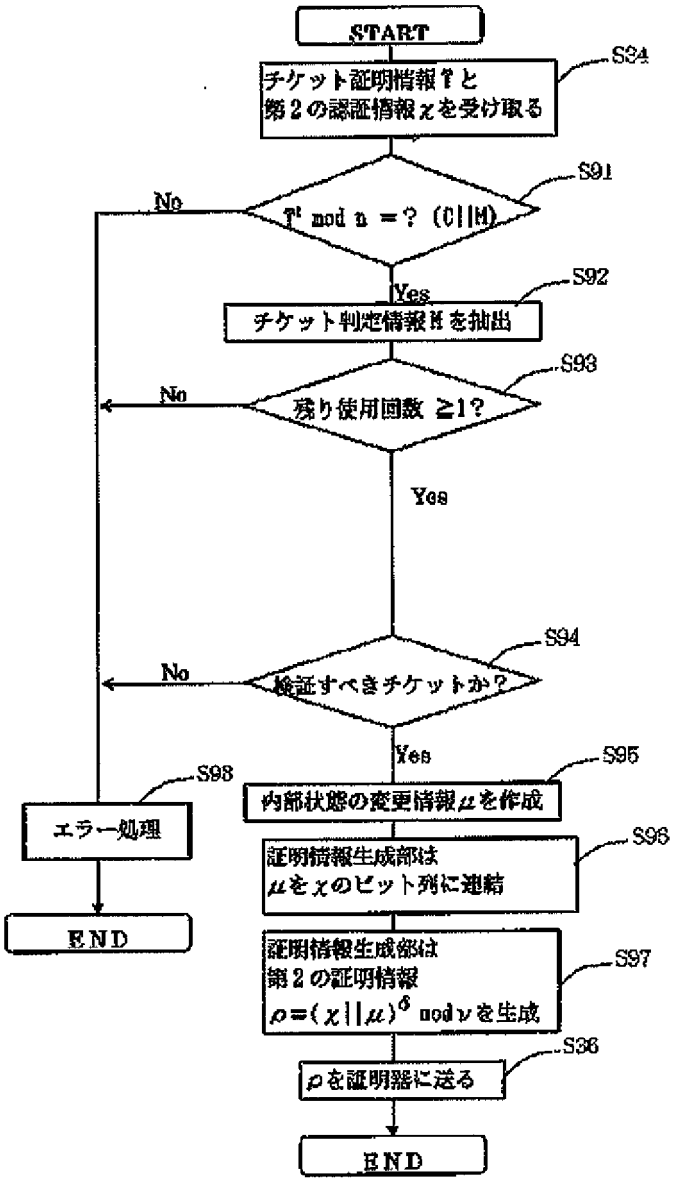

検証装置
100
105
101
104
102
106
通信部
100
実施例9の全体の構成
販売装置
206
209
205
204
207
チケット
チケット利用情報
内部状態
カウンタ
202
202a
208
200
チケット記憶装置
300

【図17】



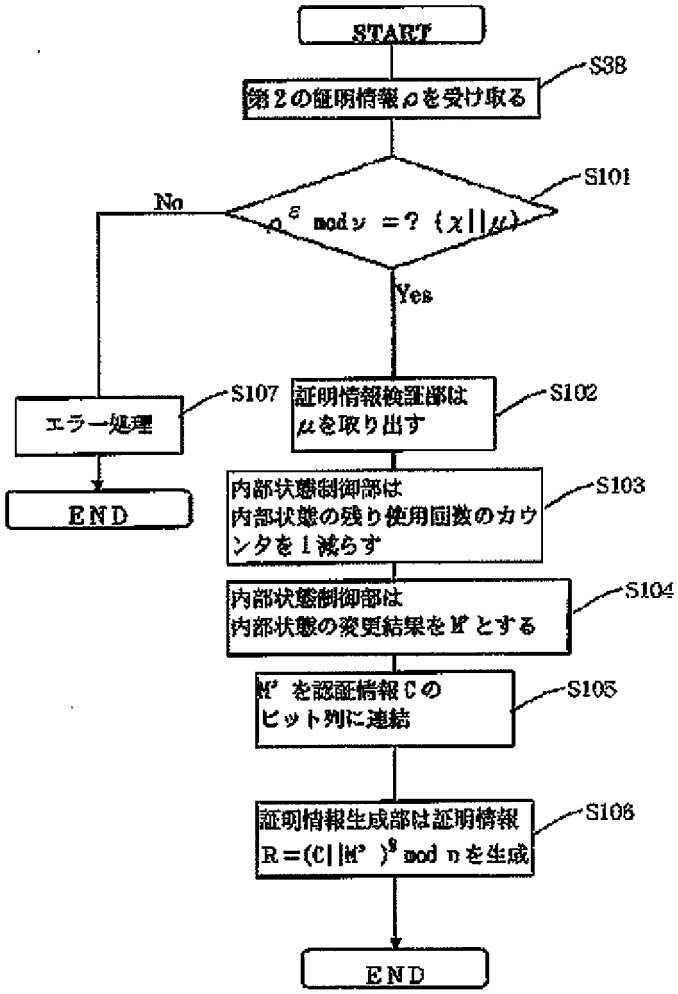
実施例3の証明装置のチケット証明情報生成処理のフローチャート

【図１８】



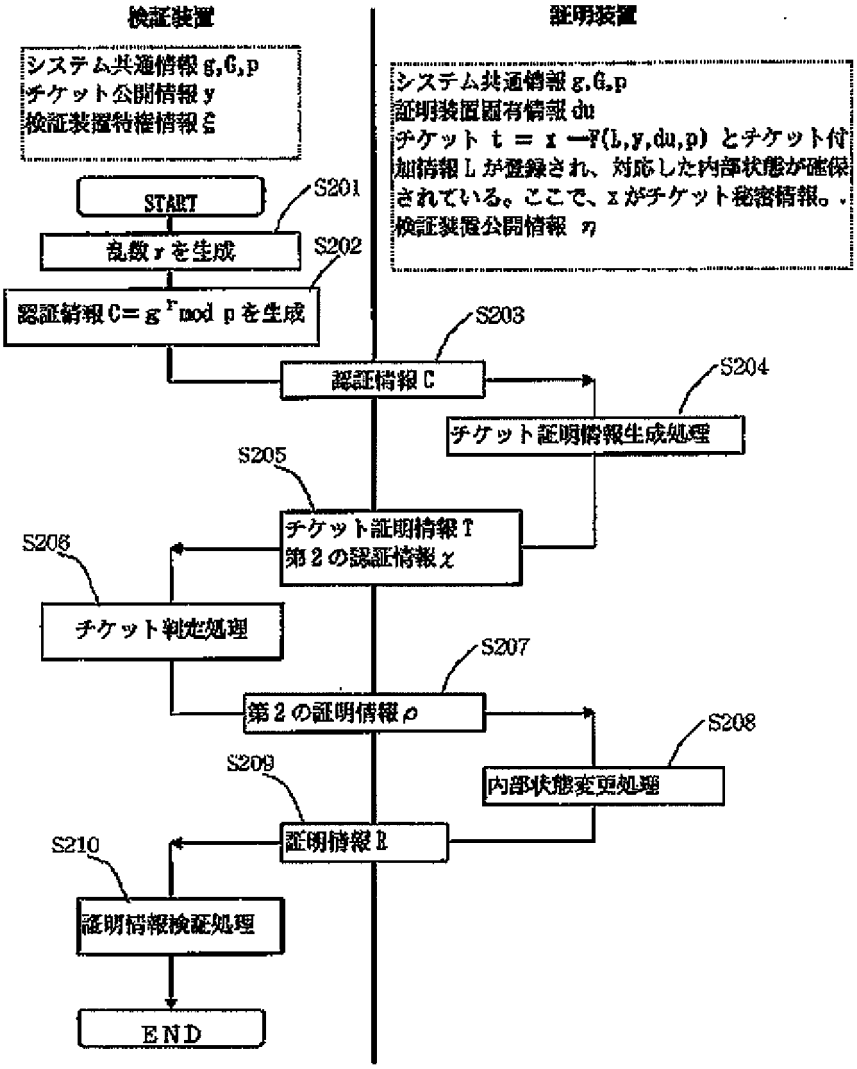
実施例３の検証装置のチケット判定処理のフローチャート

【図１９】



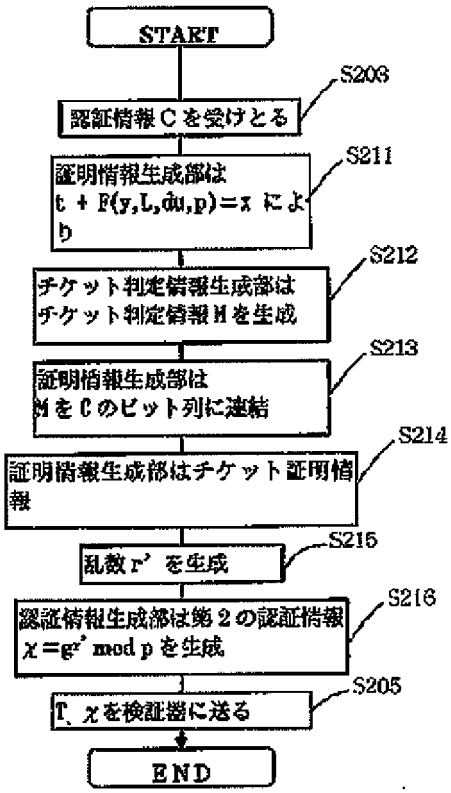
実施例３の証明装置の内部状態変更処理のフローチャート

【図２０】



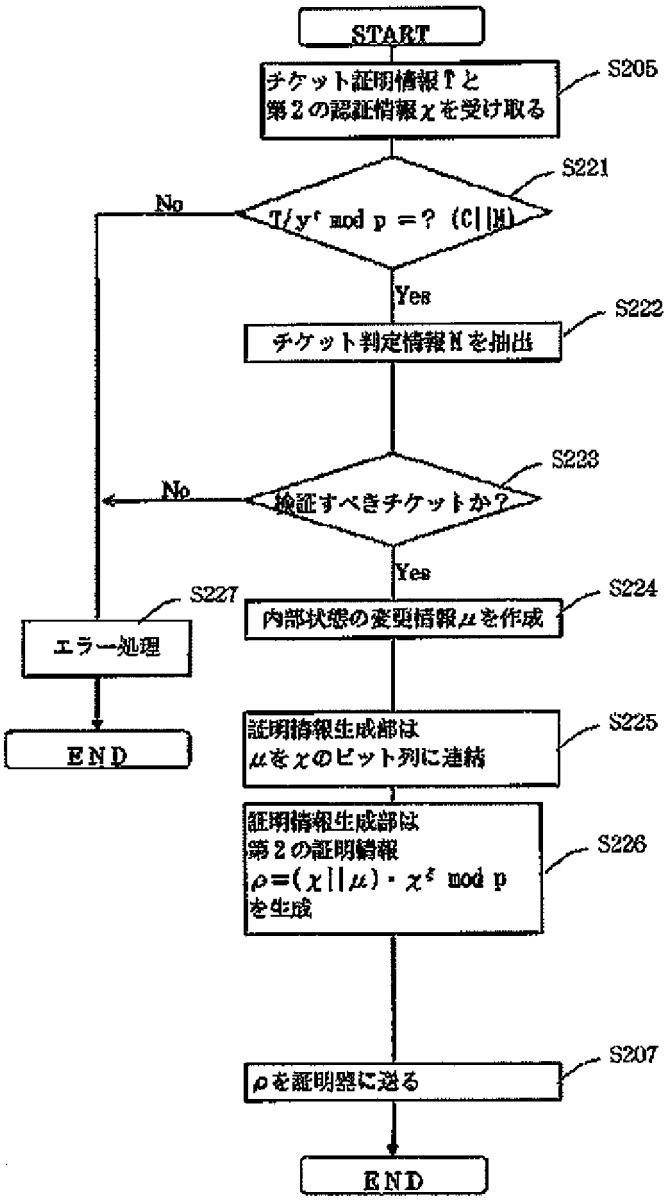
実施例４の処理全体のフローチャート

【図２１】



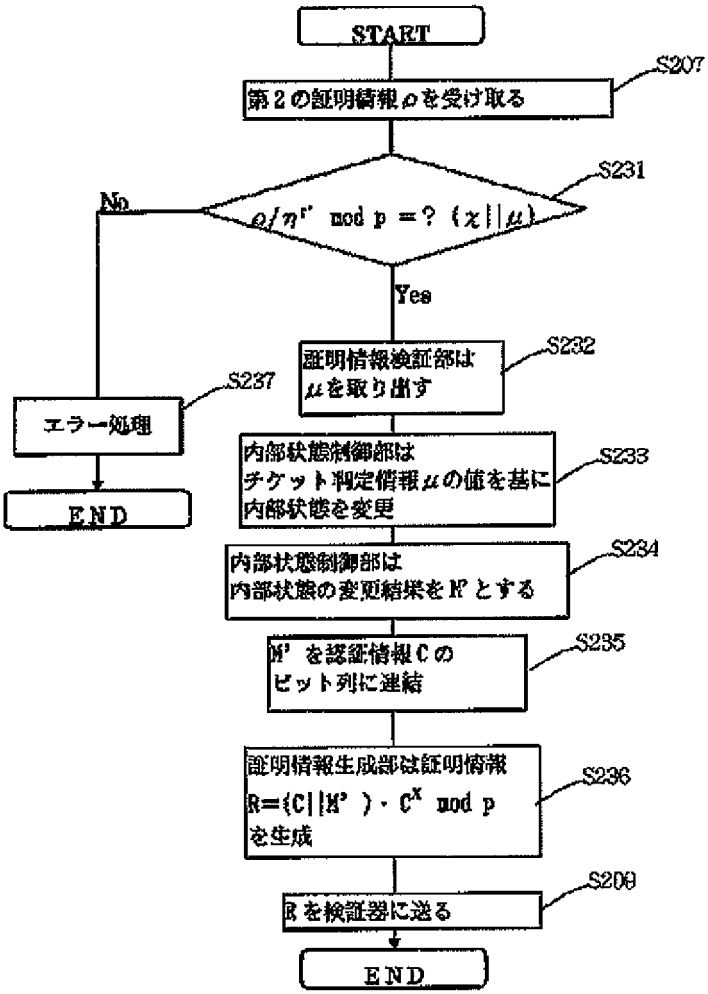
実施例４の証明装置のチケット証明情報生成処理のフローチャート

【図22】



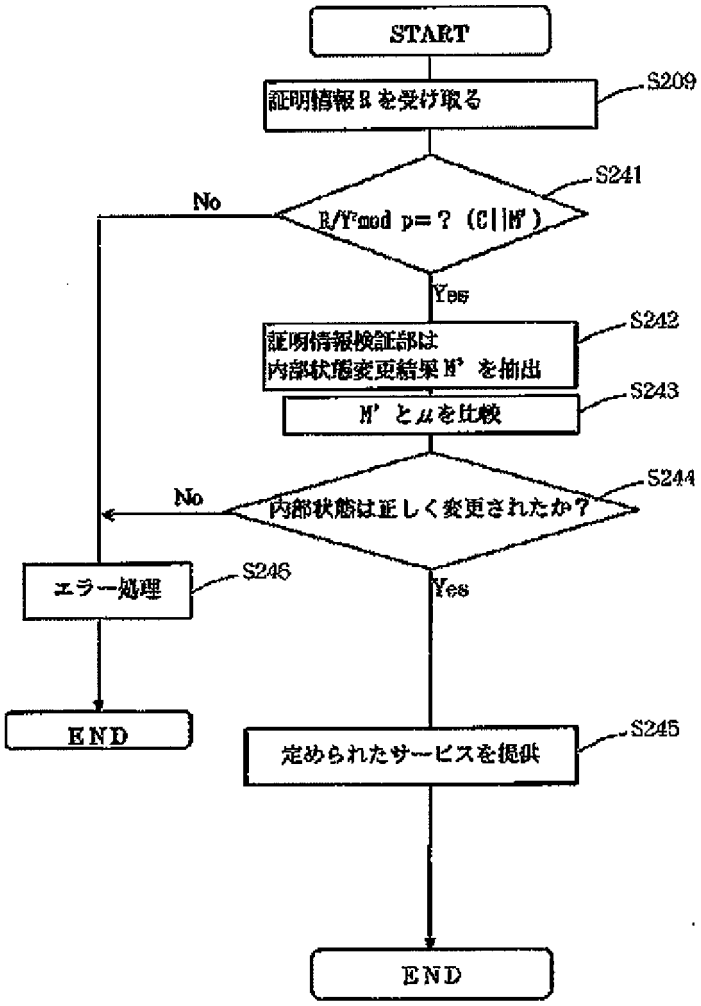
実施例4の検証装置のチケット判定処理のフローチャート

【図２３】



実施例４の証明装置の内部状態更新処理のフローチャート

【図２４】



実施例４の検証装置の証明情報検証処理のフローチャート

フロントページの続き

(51)Int.Cl.°		識別記号	FI		
G07B	1/00		G07B	5/00	C
	5/00		G09C	1/00	660Z
G07F	7/12		G06F	15/21	340C
G09C	1/00	660	G07F	7/08	C
			H04L	9/00	675Z

(72)発明者 谷口 慎一郎
神奈川県足柄上郡中井町境430 グリーンテクなかい 富士ゼロックス株式会社内